

# PassPoint *Express*

---

## **INSTALLATION and SETUP GUIDE**

---

*For Access Control Kits*

**ADEMCO  
GROUP**

N8949 4/98

### **IMPORTANT NOTICE**

This product complies with Standards of UL294 only. It has not been tested for compliance with Standards of UL1076. The burglary features of this product are only supplemental to the product's access control features. Terms used in this documentation, such as zones, perimeter, etc., are not indicative of UL approved burglary features. These terms apply only to access control applications of this product and the product's burglary features that have not been approved by UL.

## ALARM DEVICE MANUFACTURING COMPANY

A Division of Pittway Corporation  
165 Eileen Way, Syosset, NY 11791

### SOFTWARE LICENSE AGREEMENT

**You should carefully read the following terms and conditions. BY BREAKING THE SEAL ON THIS PACKAGE YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT. If you do not consent to be bound by this License Agreement, you must promptly return the unopened package to the person from whom you purchased it within fifteen (15) days from date of purchase and your money will be refunded to you by that person. If the person from whom you purchased this Software fails to refund your money, contact ADEMCO immediately at the address set out above.**

1. GRANT OF LICENSE. Subject to all terms and conditions hereof, Alarm Device Manufacturing Company, a division of Pittway Corporation ("ADEMCO") does hereby grant to the purchaser (the "Licensee") upon payment in full of the published license fee, or other license fee agreed to in writing (the "License Fee") a nontransferable, nonexclusive license to use the enclosed software ("Licensed Programs") provided herewith in Licensee's own business on a single computer for a term commencing on the date of payment in full of the License Fee and continuing in perpetuity unless terminated in accordance with the terms hereof.
2. PROPRIETARY RIGHTS. Licensee hereby acknowledges that the Licensed Programs including the algorithms contained therein are proprietary to ADEMCO. Licensee shall not sell, transfer, disclose, display or otherwise make available any Licensed Programs or copies or portions thereof to any other entity. Licensee agrees to secure and protect the Licensed Programs so as to maintain the proprietary rights of ADEMCO therein, including appropriate instructions to and agreements with its employees.
3. DOCUMENTATION. The documentation supplied with the Licensed Programs is the copyright property of ADEMCO. Licensee shall not under any circumstances divulge or permit to be divulged such documentation to any other entity.
4. COPIES. Licensee shall not copy in whole or in part the Licensed Programs or documentation provided however that Licensee shall be permitted to make one (1) copy of the Licensed Programs solely for backup purposes provided that all proprietary notices are reproduced thereon. Any such copy shall remain part of the Licensed Programs and shall be subject to this Agreement.
5. OBJECT CODE. Licensee understands and acknowledges that the Licensed Programs consist of object code only and that ADEMCO shall not supply source code versions of the Licensed Programs. Licensee shall not create or attempt to create by de-compilation or otherwise, the source code for the Licensed Programs, or any part thereof.
6. SECURITY. Licensee acknowledges that the Licensed Programs are security related and access to the Licensed Software should be limited to authorized individuals. Licensee assumes full responsibility for use of the Licensed Programs whether by authorized or unauthorized individuals. Licensee agrees that the License Fee has been set in reliance upon indemnities and the limitations on liability contained herein and that such provisions are fair and not unconscionable.
7. LIMITED WARRANTY. ADEMCO warrants that the Licensed Programs will conform to the functions described in the ADEMCO user documentation provided herewith for ninety (90) days from the date of original purchase. THE WARRANTY STATED ABOVE IS A LIMITED WARRANTY AND IT IS THE ONLY WARRANTY BY ADEMCO. ALL OTHER WARRANTIES OF MERCHANTABILITY OR WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY EXCLUDED BY ADEMCO AND WAIVED BY LICENSEE. Other than the limited warranty stated above, the entire risk as to the use, quality and performance of the Licensed Programs is with Licensee. ADEMCO does not represent that the Licensed Programs may not be compromised or circumvented; that the Licensed Programs will prevent any personal injury or property loss by burglary, robbery, fire or otherwise; or that the Licensed Programs will in all cases provide adequate warning or protection. Licensee understands that a properly installed and maintained alarm may only reduce the risk of a burglary, robbery or fire without warning, but is not insurance or a guarantee that such will not occur or that there will be no personal injury or property loss as a result. ADEMCO does not warrant that the Licensed Programs will meet Licensee's requirements or that the operation of the Licensed Programs will be uninterrupted or error free. SOME STATES DO NOT

ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE.

8. **LIMITATION OF REMEDIES.** Licensee's exclusive remedy shall be either the replacement of any diskette not meeting the limited warranty set forth above and which is returned to ADEMCO with a copy of Licensee's paid invoice or, if ADEMCO is unable to deliver a replacement diskette which is free of defects, Licensee may terminate this Agreement by returning the Licensed Programs and thereupon the License Fee shall be refunded. ADEMCO shall have no obligation under this Limited Warranty if the Licensed Programs are altered or improperly repaired or serviced by anyone other than ADEMCO factory service. For warranty service, return Licensed Programs transportation prepaid, to ADEMCO Factory Service, 165 Eileen Way, Syosset, NY 11791. ADEMCO SHALL HAVE NO LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR WITH RESPECT TO AUTHORIZED OR UNAUTHORIZED USE OF THE LICENSED PROGRAMS OR OTHERWISE WHETHER BASED IN CONTRACT, TORT OR UPON ANY OTHER LEGAL THEORY FOR CONSEQUENTIAL EXEMPLARY, OR INCIDENTAL DAMAGES, INCLUDING BUT NOT LIMITED TO LIABILITY FOR PERSONAL INJURY, PROPERTY DAMAGE, ECONOMIC LOSS, OR CLAIMS OF THIRD PARTIES, INCLUDING CUSTOMERS OF LICENSEE, EVEN IF IT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall ADEMCO's liability whether direct or indirect for any claim, under this Agreement or otherwise, regardless of cause or origin, exceed the License Fee. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSIONS OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

9. **REGISTRATION.** In order to qualify to receive notification of ADEMCO updates to the Licensed Programs, Licensee must complete and return the enclosed Registration Form to ADEMCO within twenty (20) days from date of purchase. Notwithstanding, ADEMCO is under no obligation to release updates to the Licensed Programs.

10. **TERMINATION.** Upon the breach or non-compliance with any term or provision of this Agreement, ADEMCO shall have the right to terminate the license granted hereby by written notice to Licensee. Upon such termination Licensee shall immediately turn over to ADEMCO all copies of the Licensed Programs and any documentation supplied in connection therewith. Such remedy shall be in addition to and cumulative to any other remedies ADEMCO may have at law or in equity with respect to such breach or non-compliance.

11. **GENERAL.** This agreement is the complete and exclusive statement of the understanding of the parties involved with respect to the transaction contemplated hereby and supersedes any and all prior proposals, understandings and agreements. This Agreement may not be modified or altered except by a written instrument signed by Licensee and an authorized representative of ADEMCO. Licensee may not assign or sublicense without the prior written consent of ADEMCO, its rights, duties or obligations under this Agreement to any person or entity, in whole or in part. If any provision of this Agreement is invalid under any applicable statute or rule of law it is to that extent to be deemed omitted. This Agreement and the performance hereunder shall be governed by the laws of the State of New York and the sole venue for suit shall be in an appropriate state or federal court located in the State and City of New York. The failure of ADEMCO to exercise in any respect any rights provided for herein shall not be deemed a waiver of such right or any further right hereunder. No action regardless of form arising in connection with this Agreement may be brought more than two (2) years after the date such cause of action shall have arisen. ADEMCO shall have the right to collect from Licensee any expenses incurred including attorneys' fees in enforcing its right under this Agreement.

# Table of Contents

## Section One - Setting Up PassPoint

---

- Introduction to Setup..... 1-1**
  - Understanding PassPoint Kits..... 1-2
  - System Hierarchy..... 1-3
  - What’s In Section One? ..... 1-4
  - About Your PassPoint Access Starter Kit..... 1-5
  - Installation and Setup Map ..... 1-9
    - Where do you go from here? ..... 1-10
  
- Preparing For Your Installation ..... 2-1**
  - How Should You Prepare For Your Installation?..... 2-3
    - Where will my Access Points be?..... 2-4
    - What level of security should I have for my Access Points?..... 2-4
    - What type of door control hardware should I use?..... 2-5
    - Where will my system computer be located? ..... 2-5
  - Using a Floor Plan ..... 2-5
  - Selecting Your Access Points ..... 2-8
    - Example 1 - Basic entry control ..... 2-9
    - Example 2 - Entry control with Door Status Monitoring ..... 2-10
    - Example 3 - Entry control with Door Status Monitoring and Request-to-Exit . 2-11
    - Example 4 - Entry and exit control with Door Status Monitoring..... 2-12

|                                                        |            |
|--------------------------------------------------------|------------|
| Door Control Module configuration .....                | 2-13       |
| Types of Card Readers.....                             | 2-15       |
| Where do you go from here? .....                       | 2-17       |
| <b>System Installation.....</b>                        | <b>3-1</b> |
| Mount the System Panel .....                           | 3-4        |
| Connect the System Modules .....                       | 3-5        |
| Mount and Connect Card Readers .....                   | 3-7        |
| Mounting card readers .....                            | 3-8        |
| Connecting card readers.....                           | 3-8        |
| Mount and Connect Door Strikes and Magnetic Locks..... | 3-10       |
| Mounting door strikes and magnetic locks .....         | 3-10       |
| Connecting door strikes and magnetic locks .....       | 3-11       |
| Connect the Computer Cable.....                        | 3-12       |
| Mount and Connect the Keypad .....                     | 3-13       |
| Where do you go from here? .....                       | 3-16       |
| <b>Software Setup .....</b>                            | <b>4-1</b> |
| What Is PassPoint Express? .....                       | 4-4        |
| System requirements.....                               | 4-5        |
| Install PassPoint Express .....                        | 4-6        |
| Start PassPoint Express.....                           | 4-7        |
| Create a New Account .....                             | 4-8        |
| The PassPoint Express Environment .....                | 4-10       |
| Major screen components .....                          | 4-11       |
| <b>System Configuration .....</b>                      | <b>5-1</b> |
| Run the Setup Wizard .....                             | 5-4        |
| Establish Communications .....                         | 5-7        |
| Auto Enroll Modules .....                              | 5-8        |
| Download the Database .....                            | 5-10       |

|                                                         |            |
|---------------------------------------------------------|------------|
| <b>Managing Cards and the Cardholder Database .....</b> | <b>6-1</b> |
| About the Cardholder Database .....                     | 6-2        |
| Using the Card Wizard .....                             | 6-4        |
| Adding a single card .....                              | 6-6        |
| Adding a batch of cards .....                           | 6-9        |
| Adding Cards Manually .....                             | 6-10       |
| Using the Custom tab.....                               | 6-15       |
| Using the Action tab .....                              | 6-15       |

## **Section Two - Expanding PassPoint**

---

|                                                             |            |
|-------------------------------------------------------------|------------|
| <b>Adding a Door Expansion Kit.....</b>                     | <b>7-1</b> |
| Understanding Your Door Expansion Kit .....                 | 7-2        |
| Installing the DEK .....                                    | 7-3        |
| Mount the DEK panel .....                                   | 7-3        |
| Connect the DCM .....                                       | 7-5        |
| Activate the system.....                                    | 7-6        |
| Add and set up the DCM .....                                | 7-7        |
| Auto enroll the DCM .....                                   | 7-14       |
| Download the database .....                                 | 7-15       |
| Configuring the DCM .....                                   | 7-17       |
| DCM System tab.....                                         | 7-18       |
| Access Point A/B tabs.....                                  | 7-19       |
| Skeleton RCM tab.....                                       | 7-30       |
| <b>Adding a Card Enrollment Kit.....</b>                    | <b>8-1</b> |
| Understanding Your Card Enrollment Kit.....                 | 8-2        |
| Installing the CEK .....                                    | 8-3        |
| Choose a location for the CEK .....                         | 8-3        |
| Connect the CEK to the system .....                         | 8-3        |
| Connect the power transformer and activate the system ..... | 8-4        |
| Add and set up the CEK .....                                | 8-5        |

|                                      |            |
|--------------------------------------|------------|
| Auto enroll the CPM.....             | 8-6        |
| Download the database .....          | 8-8        |
| <b>Wiring Considerations .....</b>   | <b>A-1</b> |
| Wiring Considerations .....          | A-2        |
| Topology .....                       | A-2        |
| Wiring notes.....                    | A-8        |
| Wire characteristics.....            | A-9        |
| Main Logic Board Connections .....   | A-10       |
| Door Control Module Connections..... | A-11       |
| Power supply specifications.....     | A-12       |
| <b>Glossary .....</b>                | <b>G-1</b> |



# *Section One*

---

•

## *Setting Up PassPoint*



## Chapter

# 1

## *Introduction*

This chapter provides you with an overview of the various PassPoint Access Control Kits. It also provides a full description of the PassPoint Access Starter Kit and the steps involved in getting your system installed and configured.

In this chapter you will learn about:

- **The contents of this section**
- **The contents of your PassPoint Access Starter Kit**

---

## ***Understanding PassPoint Kits***

This guide is about PassPoint Kits, the basic pre-configured PassPoint packages you will use to quickly get your system up and running. All kits are self-contained. By combining kits (and separate PassPoint modules), you can expand and build on any existing PassPoint installation.

There are three types of PassPoint kits:

- **Access Starter Kit (ASK)**

The ASK contains everything you need to get a two-door installation up and running. It is the basic building block of all PassPoint systems.

Most of this guide describes the ASK.

- **Door Expansion Kit (DEK)**

The DEK allows you to add two more doors to an already operational PassPoint system. The components of the DEK, as well as installation and configuration instructions, are provided in Chapter 7.

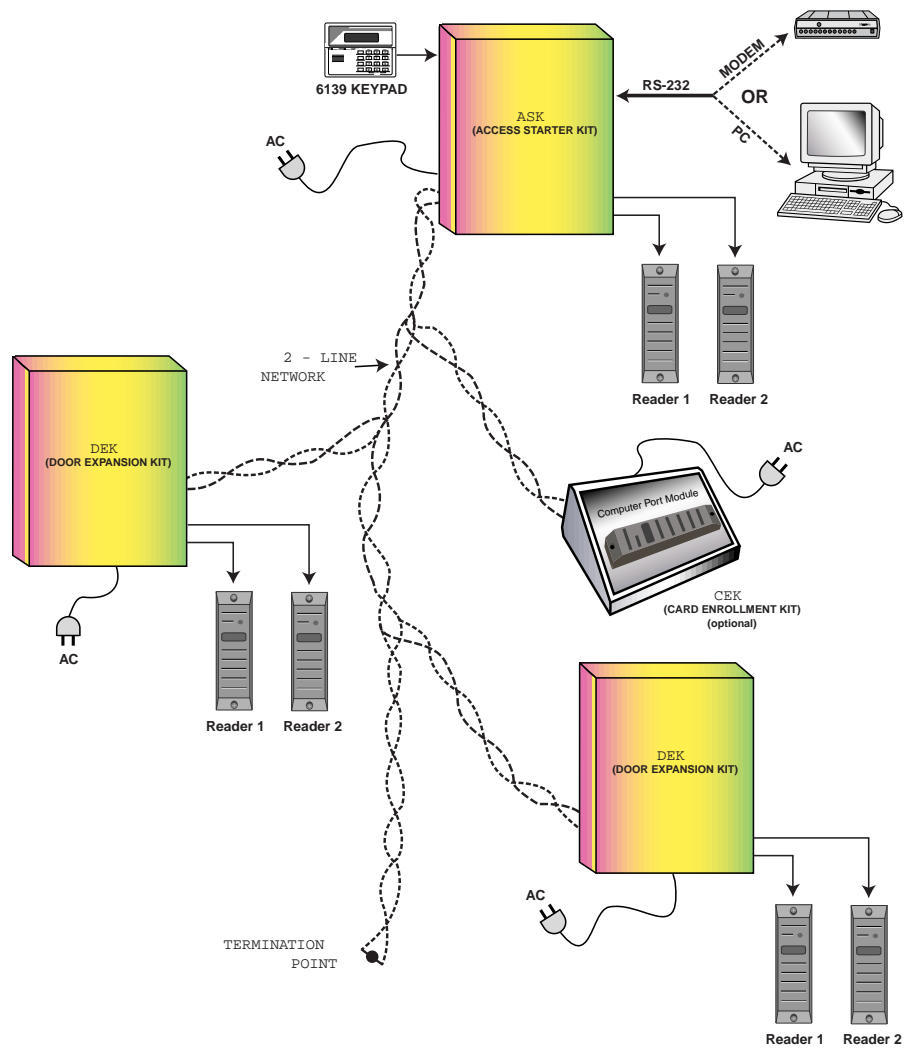
- **Card Enrollment Kit (CEK)**

The CEK is a kit that allows you to quickly enroll system ID cards. It consists mainly of a stand-alone card enrollment reader that connects directly into your existing system.

Installation and configuration instructions for the CEK are provided in Chapter 8.

## System Hierarchy

The PassPoint system is composed of kits. Shown below is an example of a basic PassPoint installation:



---

## What's In Section One?

Section One of this guide contains everything you need to get your PassPoint Access Starter Kit up and running. It will walk you step-by-step through all the procedures from installing your hardware to enrolling some test ID cards. Once you have enrolled some test cards, you can test your system to see if your system is running properly.



---

This section has been written from the perspective of a two-door system only. If you have purchased a PassPoint Door Expansion Kit or Card Enrollment Kit, refer to Section Two of this guide for complete instructions on installing and configuring these kits.

---

This section of the guide has been divided into four parts:

- **Part One - Preparing For Your Installation**

Before attempting to install the PassPoint system, there are several things preparations you should make. Proper preparation will make the task of installing the system much easier. Chapter 2 tells you how to prepare for your installation.

- **Part Two - System Installation**

Chapter 3 is the system installation section of this guide. This section tells you how to connect all of the system modules that come with your kit, including mounting the cabinet and wiring your card readers.

- **Part Three - PassPoint *Express* Installation**

PassPoint *Express* is the system interface you will be using

to configure and operate your PassPoint system. It needs to be installed on your user terminal (i.e. the PC you will be using to connect to the system's panel). Chapter 4 covers the entire installation of PassPoint *Express*.

- **Part Four - System Configuration**

After you have installed your system hardware, you need to configure the system so that it will operate properly. Most configuration options for your PassPoint Access Starter Kit have already been defaulted at the factory, but there are some configuration options that still need to be set by you, such as setting up your doors and enrolling access cards.

Configuration information begins in Chapter 5.

## ***About Your PassPoint Access Starter Kit***

The PassPoint Access Starter Kit (ASK) has been designed to be easy to install and configure. Where possible, default configuration options have been provided. If you follow the procedures in this guide, you should have no trouble getting your system operational.

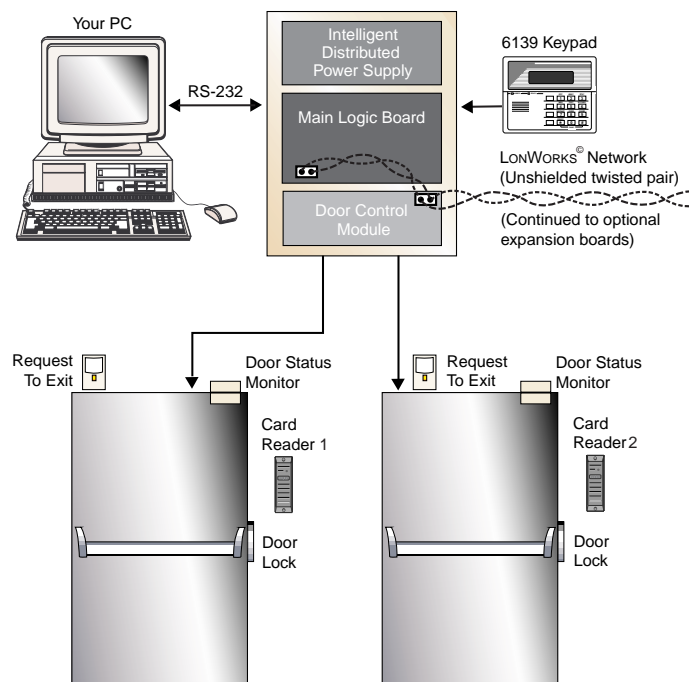
### ***What's in your kit?***

Your Access Starter Kit consists of the following hardware components:

- **1 pre-configured access panel, consisting of the following:**
  - 1 Metal enclosure
  - 1 Main Logic Board
  - 1 Door Control Module
  - 1 Power Supply

- **1 plug-in transformer**
- **2 million-mount proximity readers or 2 million-mount magnetic stripe card readers (depending on the type of reader chosen)**
- **1 6139 keypad**
- **ID cards (to be used with card readers)**
- **PassPoint *Express* software**
- **1 RS-232 cable (null modem cable)**

(Used for connecting your PassPoint panel to your user PC serial port)



**ACCESS STARTER KIT (ASK)**



**Major components**

There are four main components to your PassPoint system. They are:

**Main Logic Board (MLB)**

The MLB is the central controller of the PassPoint system. It contains the card database, the event log, and system configuration information. It also keeps track of the system status. The MLB receives its power from the PassPoint power supply, and communicates with the Door Control Module (described below) to determine if access should be granted at a particular Access Point.

**Door Control Module (DCM)**

The DCM provides all the inputs and outputs required to manage two Access Points (i.e. doors). The DCM can connect to two card readers and simultaneously accept card data from two card readers. It provides two Form C, supervised output (i.e. voltage monitored) relays which are used to operate electromagnetic door locks or door jamb-mounted lock strikes. It also provides two trigger outputs which can be used to operate sounders or LEDs.

**The PassPoint system power supply**

The PassPoint system power supply provides all the power needed by the MLB and DCM. It is connected to the AC line voltage via an 18VAC, 50VA Basler-type plug-in power transformer (supplied with your kit). The power supply provides a battery backup/charger connection and supports a 7AmpHour battery (not supplied).

Connection information and specifications for the power supply can be found in Appendix A, as well in the Summary of Connections diagram at the end of this guide.

### **The PassPoint *Express* system interface**

PassPoint *Express* is a Windows 95 software program that allows the PC to communicate with the Main Logic Board of the system. You will be using PassPoint *Express* to configure the system. After the system is up and running, the system operators will be using PassPoint *Express* to operate PassPoint.



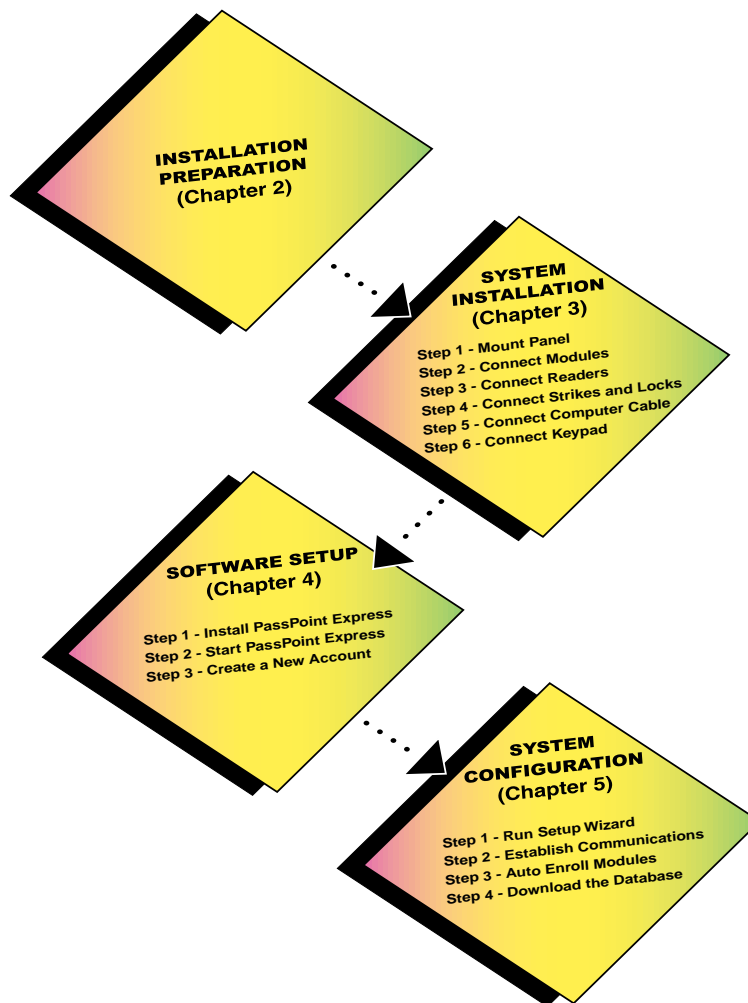
---

The Passpoint *Express* system interface requires a PC. The PC is used to configure and operate the system, although the PC is not necessary for the system to run unattended. Also, if you are running PassPoint *Express* remotely, you will need at least one modem to connect the PC with the PassPoint system. Both the PC and modems are considered accessories and are not included with your PassPoint Access Starter Kit.

---

## Installation and Setup Map

Below is a depiction of all the steps that must be taken to get your PassPoint system up and running. The steps are broken down into parts. Each part is covered in detail in a different chapter of this guide.



## ***Where do you go from here?***

Begin by preparing for your installation. Instructions for preparation are included in the next chapter. Here you will see how to use a floor plan to determine your system layout, and will be prompted with some important questions that must be considered before you can proceed with installing your system.

## Chapter

# 2

## *Preparing For Your Installation*

Before attempting to install the PassPoint system, there are several things you should do to prepare for your installation. Proper preparation will make the task of installing the system much easier.

In this chapter you will learn:

- **How PassPoint can be installed to suit your individual needs**
- **How to select and configure the Access Points for your system**
- **How to place your system components**
- **What steps must be performed for hardware installation**



## ***How Should You Prepare For Your Installation?***

With PassPoint, proper preparation is essential to a sound, problem-free installation. It involves knowing your site and its Access Points, and knowing the level of security desired for each point. It also involves the proper placement and utilization of system hardware.

Because the system is so flexible, it allows you to install its components in multiple ways. There are, however, several things common to each installation, such as Access Points and hardware. These common configuration issues are a good place to start when preparing for your own installation.

### ***Understanding Access Points***

PassPoint defines Access Points beyond the conventional definition of a simple door. An Access Point represents a collection of objects (i.e. resources) that allow entry/egress through a portal. These objects include the hardware related items (readers, locks, etc.) as well as software functions that parameterize the Access Point (schedules, cardholders, etc.).

### ***Ask yourself some basic questions***

A good approach to preparing for your installation is to ask questions about the site into which PassPoint is being installed. Answering these questions will help you determine the type of hardware you need, where it should be placed, how it should be wired, etc. Then, after you've installed and wired your system hardware, you will be able to configure it using one of the system's interfaces.

Below are some of the questions that you will need to answer before you can begin your installation. It should be noted that these questions pertain to a general installation. Because of the

flexibility of PassPoint, it is impossible to foresee and describe every possible installation scenario. But when used as a general guide, the answers to these questions will have you well on your way to a successful PassPoint installation.

### ***Question 1 - Where will my Access Points be?***

This is perhaps the most important consideration when preparing for your installation. Access points, or doors, control the entry and egress from a premises, as well as the flow of traffic within the premises. You will have to determine which doors you want to control.

See the section of this chapter titled '*Selecting Your Access Points*' for instructions on choosing your system's Access Points.

### ***Question 2 - What level of security should I have for my Access Points?***

Security levels for Access Points can vary, depending on what type of system hardware the Access Point has and how it is configured. You can have a door with only a card reader, or with a card reader/keypad combination. The door can be monitored for its status, or it can simply be allowed to stay open unconditionally. Many other security level options are also available.

See the section of this chapter titled '*Selecting Your Access Points*' for information regarding Access Point security levels.



**Question 3 - What type of door control hardware should I use?**

The type of door control hardware you should choose depends in part on the level of security you want for each Access Point. As stated above, you can have doors that have only a single card reader, or you can have card reader/keypad combination units requiring an occupant to enter a PIN code after swiping his/her card. There are many types of door control hardware available, as well as different ways to configure them.

**Question 4 - Where will my system computer be located?**

You must determine where the computer running your system software will be located. You are not limited by physical distance, since the Main Logic Board of the system can communicate to your system interface via modem, if you wish.

## ***Using a Floor Plan***

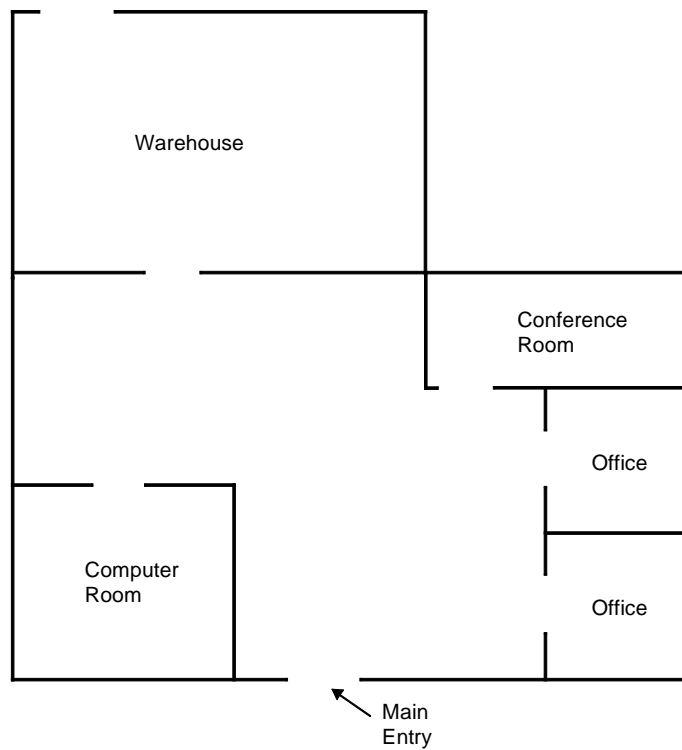
When preparing for your PassPoint installation, it is strongly recommended that you obtain a floor plan of the installation premises, if possible. A floor plan will allow you to visualize your installation and help you to determine your Access Points and hardware location. A floor plan can be any blue print or design plan showing the “foot print” (i.e., the top view) of the premises.

If you are unable to obtain a floor plan of the premises, you can simply draw one yourself. It doesn't have to be anything elaborate, just a simple aerial view of the building showing its doors and rooms scaled to their approximate dimensions.

Dimensions are important because there are wire length considerations that must be kept in mind when wiring together the system hardware.

Here is an example of a simple floor plan:

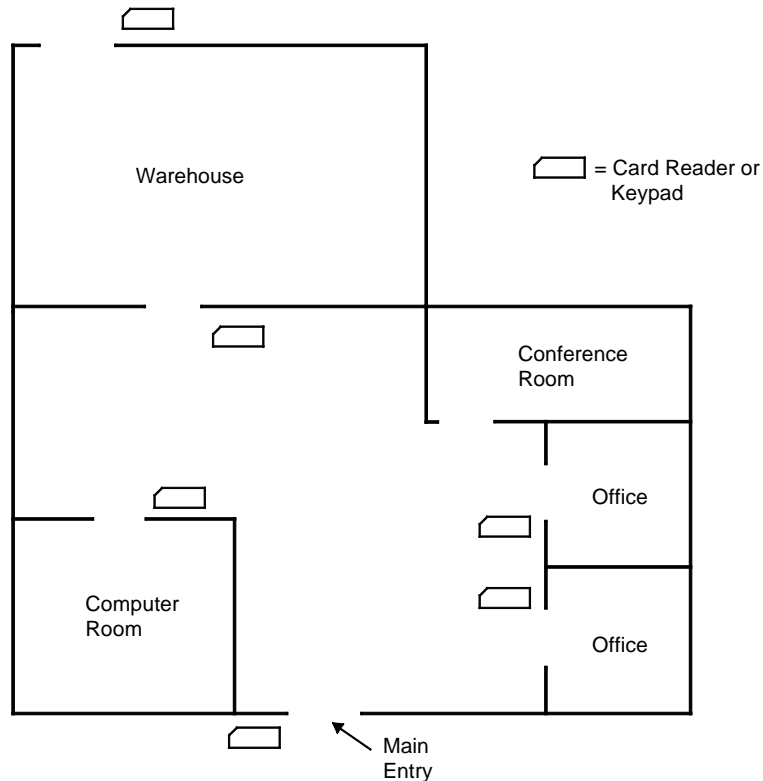
*Here's a business office without PassPoint installed. Note that every room is accessible to everyone.*



Of course, your own floor plan may be much more extensive than this one, but the principles involved are the same. You have a premises with a main entry/exit door, and the premises contains other rooms and facilities that must also be protected.

Now with this floor plan in hand, you can decide what you want to protect and how to do it:

*That same premises with PassPoint installed now controls the flow of people between rooms.*



In the case of this PassPoint installation, you can see that most of the rooms of the premises have been protected with a card reader (or keypad). The conference room, however, has been left unprotected by the PassPoint system, since it needs to be accessed by everyone at any given time. It should be noted again that although the floor plan above shows the use of card readers or keypads, these devices could just have easily been combination (card reader with keypad) units.

---

## Selecting Your Access Points

The first step in preparing to install your PassPoint system is to select your Access Points. Simply put, Access Points are the doors that people will use to enter and exit the premises being controlled. Once you've chosen what doors you want monitored, you can then decide the level of access control you want for each. This will determine the type of hardware needed for each Access Point.

### ***Access point configurations can vary***

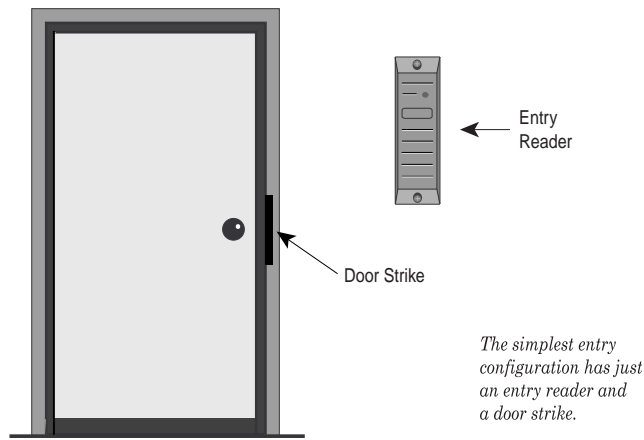
Each Access Point can be configured in several different ways. Each way provides a different degree of security and can enforce a direction of passage through the Access Point.

Remember that an Access Point is really a combination of system resources (i.e., card readers, door control relays, and protective zones). The way you combine these resources determines the level of security for the Access Point. It also determines whether the Access Point is a Door Status Monitor (DSM) zone or a Request to Exit (RTE) zone. DSM and RTE are the two kinds of protective zones. An Access Point can be one of these zone types, both types, or neither.

Below are some sample Access Point entry control configurations. They range from very simple (and consequently less secure) to fairly elaborate.

### **Example 1 - Basic entry control**

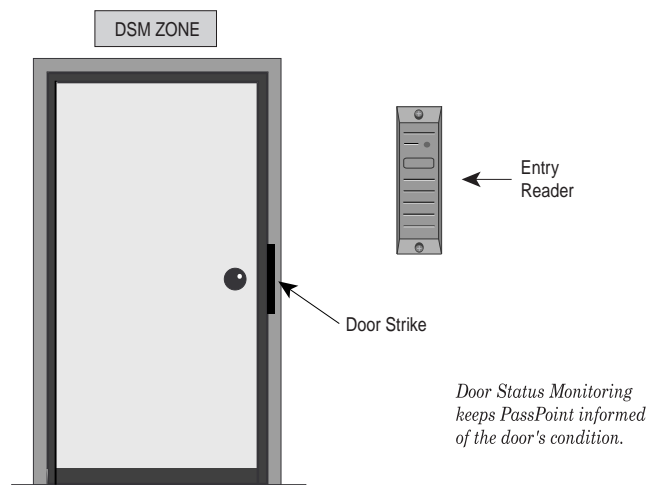
The simplest configuration for entry control is to have an entry reader and a door control relay positioned at the Access Point:



In this configuration, the occupant swipes his/her ID card at the card reader to gain entry to the Access Point. The reader reads the data on the card and PassPoint determines whether or not to grant access to the occupant. If access is granted, the door control relay at the Access Point is energized and the door strike is unlocked, allowing the occupant to enter.

## ***Example 2 - Entry control with Door Status Monitoring***

Here is the same configuration as Example 1, only with Door Status Monitoring added:



As its name implies, Door Status Monitoring allows the system to constantly monitor the Access Point for any change in its status. It lets the system know when the door has been forced open or when it has been held open longer than normal after access has been granted. Without DSM, as in Example 1, the system only determines whether or not to grant access. It does not monitor the status of the Access Point for anything unusual.

### **Example 3 - Entry control with Door Status Monitoring and Request-to-Exit**

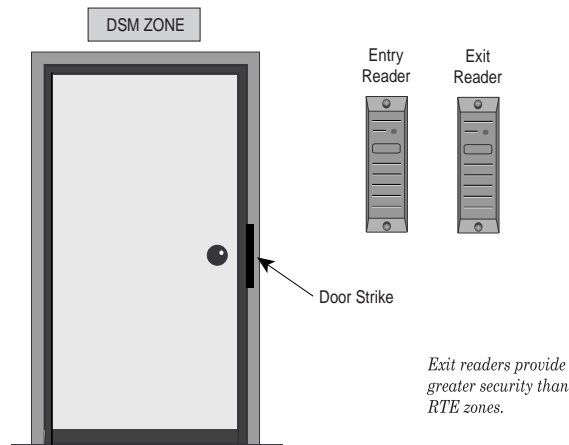
Add Request-to-Exit to an Access Point, and you can control when to allow occupants to exit:



RTE zones allow the system to understand when the Access Point's door is to be unlatched so that an occupant may exit. The device used for RTE can be a button that the occupant must push to exit, or it can be an infra-red device that automatically detects when an occupant is near the door. In either case, the device is always mounted on the protected side of the Access Point.

### **Example 4 - Entry and exit control with Door Status Monitoring**

For added security, an exit reader can be added to the Access Point:



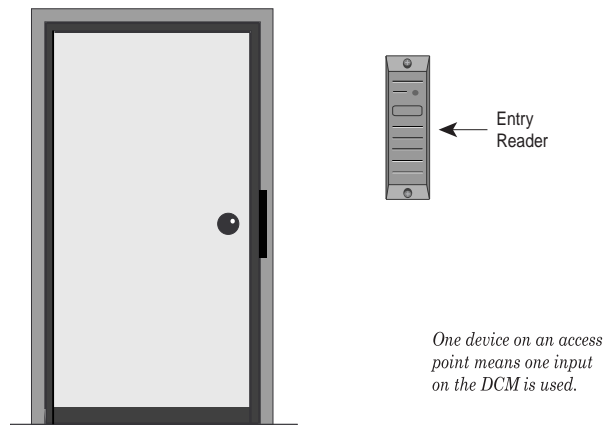
When an Access Point has an exit reader, occupants must “swipe out” in order to exit. That is, they will have to show the system their card again. Unlike the RTE zone described in Example 3, this configuration directs the system to be very selective about who it allows to exit. Only occupants with a valid ID card may exit through the Access Point.



## **Door Control Module configuration**

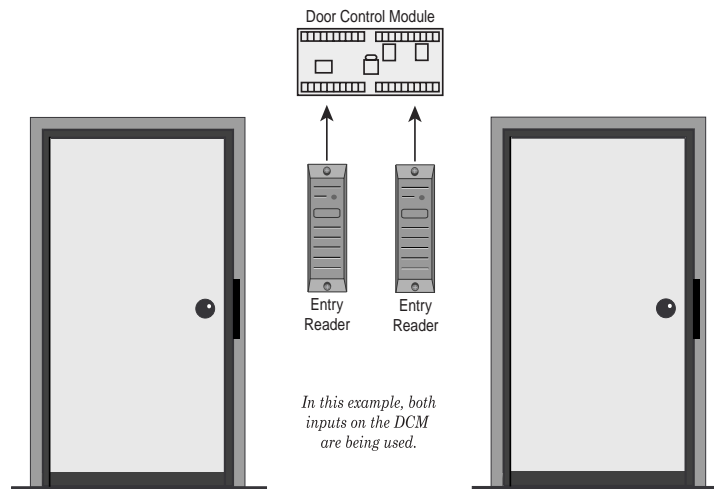
Because each DCM has inputs and outputs for only two devices (i.e., card readers, keypads, or combination units), these limitations must be kept in mind when planning your installation. Specifically, which doors do you want to control and how do you want to control them?

Consider again the Access Point examples given in the previous sections. In the first example, we have a basic entry control system with a single card reader:



In this example, since there is only one device (i.e., a reader) assigned to the door, the DCM used for the Access Point still has one input remaining.

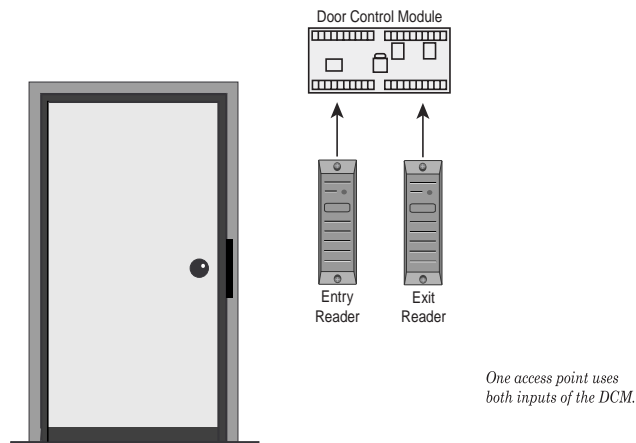
Therefore, this DCM can be used to manage another door (provided that door also has only one device), as in the diagram below:



If an Access Point has two devices on it, both inputs of the DCM are required. There are a number of times when this will be the case, and you must be aware of them in order to plan your installation properly.

*For example, if you have an Access Point that requires both an entry reader and an exit reader, you will need to wire both devices to the inputs of the DCM. This will require using the entire input capacity of the DCM.*

This example is illustrated below:



When you install your DCMs, you will have to remember the limitations described above. Knowing how DCMs can be configured directly relates to how many DCMs you will need and where to position them.

## ***Types of Card Readers***

With PassPoint, there are several types of card readers that can be used throughout the system. You have already seen two of the reader types (entry readers and exit readers) used in the examples in the previous section. Each PassPoint reader type is explained below:

**Entry readers** - These readers are used to control entry to an Access Point. The Cardholder swipes his/her card at the reader to gain entry. The reader reads the data on the card and the system determines if access should be granted. If access is

granted, the door is unlocked for a specified period of time (defined by the installer) and the Cardholder can open the door.

**Exit readers** - Exit readers work nearly identically to entry readers, except that they are used to control egress from an Access Point.

**Command readers** - These are readers that are used to perform specific functions, or “commands.” For instance, a command reader might be positioned in the front hall of a building within easy reach of someone coming through the front door. When the Cardholder swipes his/her card at the reader, the lights for the building might go on. The card swipe does not unlock the door. Instead, an event/action relationship has been set up between the Cardholder’s card and the reader.

All card readers, no matter what their function in the system, connect directly to Door Control Modules. The only exception to this is enrollment readers. Enrollment readers can connect to a Door Control Module, or they can be connected directly to a Computer Port Module (CPM). The CPM has a built-in card reader used specifically for card enrollment.

The function that a reader performs is set during module configuration after the reader has been connected to a DCM. When you configure a DCM, the system will ask you about the reader(s) connected to the module. You then tell the system which function you want the reader to perform.

***Committed and uncommitted readers***

All readers, no matter what their function, fall within two main categories: committed and uncommitted.

- **Committed Readers**

Committed readers are readers directly associated with Access Points. That is, they control entry or exit through a door. These readers can be straight entry readers, entry with door status monitoring, straight exit, etc. The committed reader is the most common type of reader in an installation, and is the one that most Cardholders will be familiar with. The Cardholder swipes his/her card at a committed reader to gain entry or egress through a door.

- **Uncommitted Readers**

Uncommitted readers are NOT associated with Access Points. Although they connect to DCMs just as committed readers do, they do not control entry or egress through doors. Uncommitted readers can either be command readers or enrollment readers.

## ***Where do you go from here?***

Now that you have made the proper preparations, you can begin installing your system. Full instructions for installing your system are included in the next chapter. Here you will see how to mount the PassPoint panel and make all the connections necessary for your system to function properly.



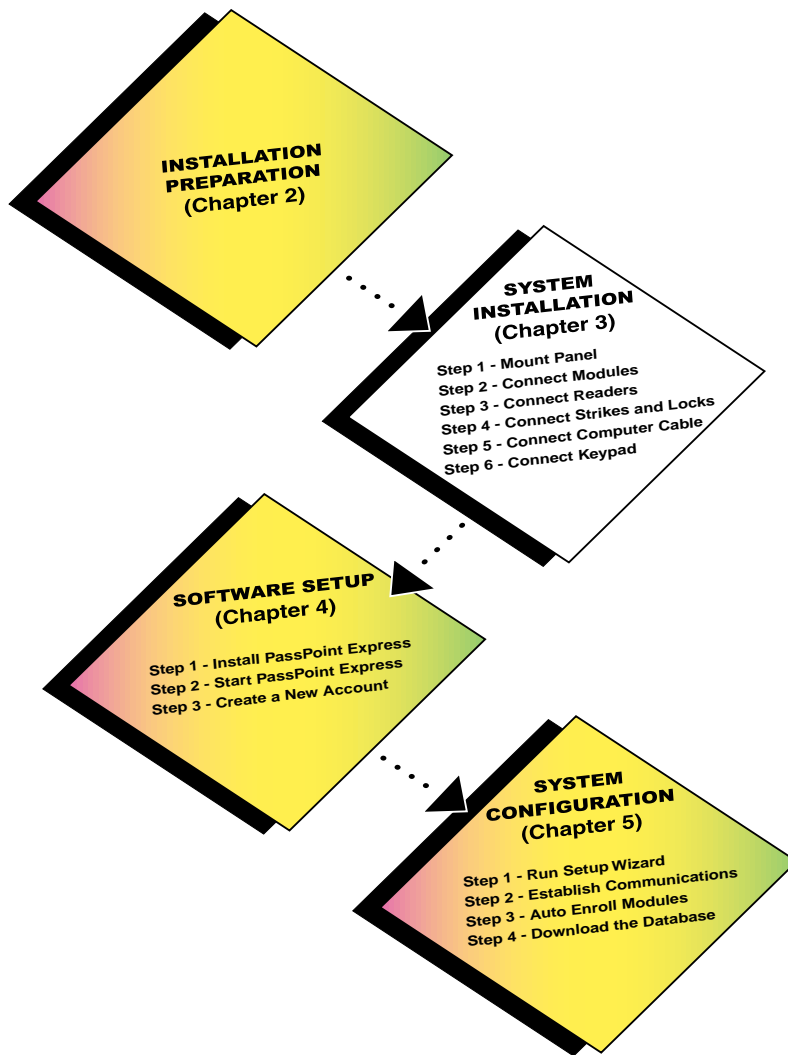
Chapter

# 3

## *System Installation*

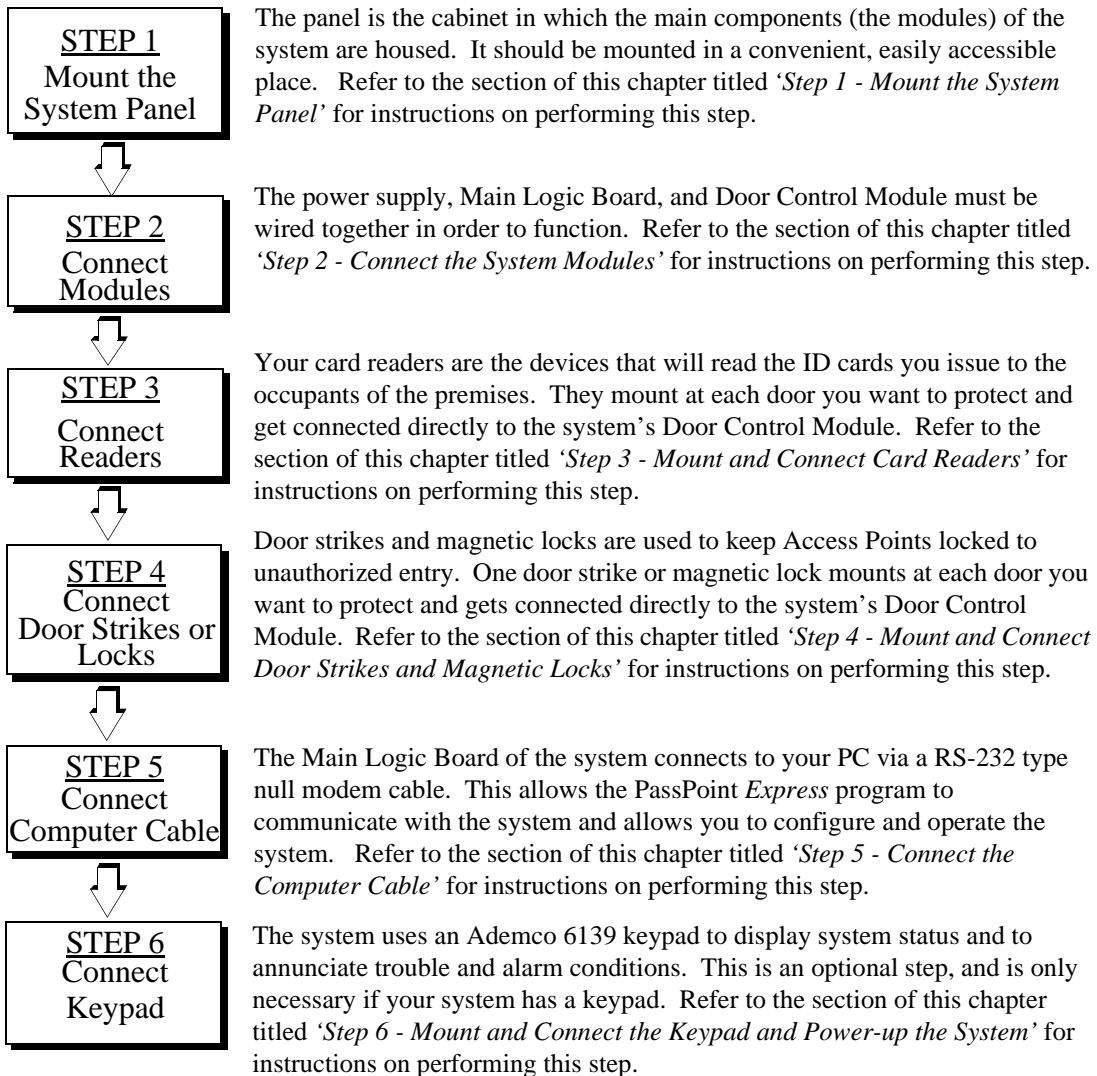
This chapter shows you how to install and wire your PassPoint system. In this chapter you will learn how to:

- **Mount the system panel**
- **Connect your card readers**
- **Connect your door strikes or magnetic locks**
- **Connect the system's RS-232 computer cable**
- **Mount and connect the system keypad**





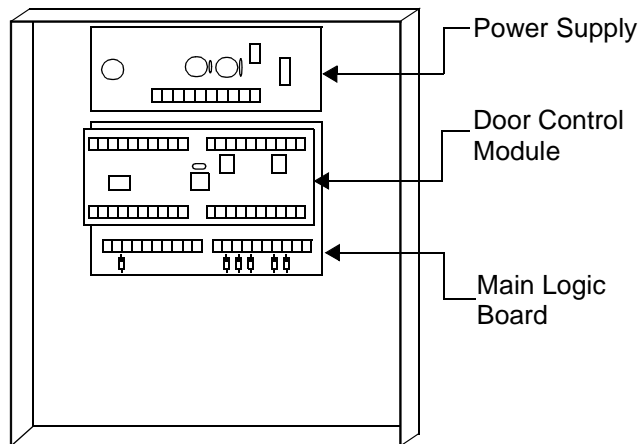
Below is a list of all the steps you must perform in order to install your PassPoint system. Each step is covered in detail in this chapter. Follow each step in order, referring to the applicable section of this chapter:



## **Step 1 - Mount the System Panel**

The ASK panel (or cabinet) contains all of the modules of the PassPoint system. All of the modules have been pre-mounted and await cabling. When the door to the panel is removed, the inside of the cabinet looks like this:

*Panel with MLB,  
DCM and power  
supply.*



### **Choosing a mounting area**

When selecting a mounting area for the panel, choose a clean, dry place not readily accessible to the general public but convenient enough so that a technician can get at the panel easily. The panel should be mounted on a sturdy wall using fasteners or anchors (not supplied in your kit). Also, the panel needs to be mounted near a suitable AC outlet and the system's PC. Refer to Appendix A of this guide for applicable wiring distance parameters.

To mount the panel, follow the procedure below:

- 1. Position the cabinet on the wall and use the holes in the back of the cabinet to mark your four mounting holes.**
- 2. Using four anchors or fasteners, mount the cabinet to the wall.**



---

When mounting the cabinet, be very careful not to jar the system's PC boards. Also, be careful not to accidentally pull off any of the wires connecting the modules. If any of the wires do come loose, re-connect them according to the Summary of Connections diagram at the end of this guide.

---

## ***Step 2 - Connect the System Modules***

Connecting the system modules within the cabinet actually involves three steps:

- **Connecting the MLB to the power supply**
- **Connecting the DCM to the MLB and power supply.**
- **Connecting the MLB ribbon cable**



---

When making these connections, refer to the PassPoint Access Starter Kit Summary of Connections diagram. You can also refer to Appendix A, Wiring Considerations, for additional diagrams and system ratings.

---

**Connect the MLB to power supply**

1. **Connect the leads of the wall pack power transformer to terminals 1 and 2 of the power supply.**

Attach the black lead to terminal 1, and the red lead to terminal 2.

2. **Connect the local power jumper between power supply connector J1 and MLB connector J1.**

This is the most common way of connecting the MLB to the power supply. However, if you do not want to use the jumper, you can connect the local power from the power supply to the MLB using wire runs between the terminal strips. (Refer to the Summary of Connections diagram for applicable terminal numbers.)



---

When making all system connections, be sure that leads are secure in their terminals and not frayed or touching other components on the panel.

---

**Connecting the DCM to the MLB and power supply**

1. **Connect the *remote* power jumper between power supply connector J5 and DCM connector J1.**

Remote power supply power (i.e. J5) is used for powering DCMs when the DCM is mounted in a cabinet with a Main Logic Board. If you are wiring a DCM mounted in a cabinet with a dedicated power supply, use the local power supply output instead (i.e., J1).

2. **Connect two network connection leads between the MLB and DCM.**

Connect one lead between terminal 1 of the DCM and terminal 16 of the MLB.

Connect the other lead between terminal 2 of the DCM and

terminal 15 of the MLB.

***Connect the MLB ribbon cable***

The system comes with a nine-pin ribbon cable used to connect the MLB to the computer cable. One end of this cable gets connected to the MLB. The other end gets mounted onto the cabinet, so that the computer cable can be plugged into it.

**1. Connect the RS-232 ribbon cable to the nine-pin connector on the right side of the system cabinet.**

The RS-232 ribbon cable allows communication between the MLB and the system PC.

**2. Secure the ribbon cable to the cabinet, using hardware supplied.**

There is a round opening with two screw holes in the right side of the cabinet for securing the ribbon cable connector.

## ***Step 3 - Mount and Connect Card Readers***

Your PassPoint Access Starter Kit comes with two card readers. Each card reader gets mounted near an Access Point (i.e., door) and is wired directly to your system's Door Control Module (DCM). A single DCM has input connections for two readers. Therefore, one DCM can control two doors.

First, you will need to mount your readers at your Access Points. After they have been mounted, you can connect them to your DCM. The instructions for performing both procedures are included in this section.



Specifications and connection information for the PassPoint power supply can be found in Appendix A, as well in the Summary of Connections diagram at the end of this guide.

---

### ***Mounting card readers***

- 1. Using the reader as a drilling template (supplied with the readers), drill two holes in each mounting wall for the readers.**
- 2. Using the reader mounting hardware included with the readers, secure the readers to the wall.**

### ***Connecting card readers***

Once the card readers are mounted, you can connect them to the system. To do so:

- 1. Wire the leads from card reader #1 to the applicable terminals of the DCM.**

Use the chart below to connect the colored leads from the card reader to the specified terminals of the DCM:

| Lead from Reader 1     | To DCM Terminal # |
|------------------------|-------------------|
| Orange (LEDRDRA)       | 11                |
| White (Data 1 (Data))  | 12                |
| Green (Data 0 (Clock)) | 13                |
| Black (Ground)         | 14                |

| Lead from Reader 1 | To DCM Terminal # |
|--------------------|-------------------|
| Red (+5VDC)        | 16                |



The readers included with the kit have nine leads, but only five of them are used and need to be wired. The other four leads (blue, brown, yellow, purple) are not used and does not need to be connected.

---

**2. Wire the leads from card reader #2 to the applicable terminals of the DCM.**

Use the chart below to connect the colored leads from the card reader to the specified terminals of the DCM:

| Lead from Reader 2     | To DCM Terminal # |
|------------------------|-------------------|
| Green (Data 0 (Clock)) | 20                |
| White (Data 1 (Data))  | 19                |
| Orange (LEDRDRB)       | 18                |
| Black (Ground)         | 17                |
| Red (+5VDC)            | 16                |

## ***Step 4 - Mount and Connect Door Strikes and Magnetic Locks***

Door strikes and magnetic locks are used to keep Access Points locked against unauthorized entry. One door strike or magnetic lock mounts at each door you want to protect. Door strikes and magnetic locks receive their power from the PassPoint power supply through the output relays of the DCM.



---

The PassPoint Access Starter Kit does not ship with door strikes or magnetic locks. PassPoint can support most types of door locking hardware compatible with the system's power supply specifications. This hardware can be purchased from any reputable dealer of security hardware.

Also, be sure to keep any documentation accompanying this hardware. You will need to refer to it for mounting and connection information.

---



---

It is recommended to use an electric suppressor such as EL-EDS (manufactured by EDCO) to provide transience protection for magnetic locks/door strikes and relay contacts. Install the suppressor across the leads connected to the lock.

---

### ***Mounting door strikes and magnetic locks***

The procedure for mounting door locking hardware varies with the type of hardware you plan to use. Refer to the documentation accompanying your door strikes or magnetic locks for instructions on performing this step.



## **Connecting door strikes and magnetic locks**

To connect a door strike or magnetic lock, follow the procedure below and refer to the PassPoint Access Starter Kit Summary of Connections diagram.

**1. Wire the door strike output of the power supply to the common terminal of the DCM output relay.**

The door strike output of the power supply is terminal #7.

The common terminal of the DCM output relay is terminal #29 for door A, terminal #24 for door B.

**2. Wire the normally open (N.O.) or normally closed (N.C.) terminal of the relay to the door strike or magnetic lock.**

If you are wiring a door strike, use an N.O. terminal. The N.O. terminals are #28 for door A, #23 for door B.

If you are wiring a magnetic lock, use an N.C. terminal. The N.C. terminals are #30 for door A, #25 for door B.

**3. Wire the door strike or magnetic lock to the ground terminal of the power supply (terminal #8).**

---

## Step 5 - Connect the Computer Cable

The PassPoint controller connects to your system interface (i.e., PC) via an RS-232 cable. The cable goes from the system's MLB to an available COM port on your computer.



---

The RS-232 cable supplied with the PassPoint Access Starter Kit can connect directly between the MLB and PC. If you intend to use a longer cable, however, you will need to purchase a “null modem” cable. Specifically, you will need a cable that swaps pins #2 and #3. Make sure when purchasing a null modem cable that these are the pins being swapped, as not all manufacturers' null modem cables are the same.

---

To connect the RS-232 computer cable:

**1. Connect the 9-pin side of the cable to the MLB.**

If you are using a PassPoint Access Starter Kit, there is a connector on the right side of the cabinet for the 9-pin side of the cable.

**2. Connect the other end of the cable to the available COM port of your PC.**

Remember which COM port you have plugged the system into. You will need to know the COM port number when you configure your system.

| MLB RS-232 Port J2 | Description | DB-9 Male Connector on side of Cabinet |
|--------------------|-------------|----------------------------------------|
| Pin 1              | DCD IN      | 1                                      |

| MLB RS-232 Port J2 | Description | DB-9 Male Connector on side of Cabinet |
|--------------------|-------------|----------------------------------------|
| Pin 2              | DSR IN      | 6                                      |
| Pin 3              | RXD IN      | 2                                      |
| Pin 4              | RTS OUT     | 7                                      |
| Pin 5              | TXD OUT     | 3                                      |
| Pin 6              | CTS IN      | 8                                      |
| Pin 7              | DTR OUT     | 4                                      |
| Pin 8              | RI IN       | 9                                      |
| Pin 9              | Ground      | 5                                      |
| Pin 10             | N/C         | N/C                                    |

## ***Step 6 - Mount and Connect the Keypad and Power-up the System***

The PassPoint system uses a standard Ademco 6139 alphanumeric keypad (supplied with the ASK) to display system status and to annunciate trouble conditions such as door-open time-out alarms. The keypad can be mounted on the wall beside the main system cabinet or can be mounted directly on the cabinet. Either way, the keypad should be mounted in an area where its display can be seen quickly and its audible signal can be heard. Only one keypad can be used with the PassPoint system.



---

The information provided in this section is only to get the system keypad up and running. Additional information about the keypad can be found in the installation instructions provided with the 6139 keypad.

---

### ***Keypad wiring and installation***

The keypad should be mounted on or near the cabinet only, and not wired through the premises. Use 22 AWG wire, to a maximum distance of 3 feet.

- 1. Remove the case back from the keypad by pushing down on the two snaps at the top of the case.**
- 2. Route wiring from the PassPoint control panel through the opening in the case back.**
- 3. Mount the case back to the wall or cabinet face.**
- 4. Plug the supplied flying lead connector into the keypad PC board.**
- 5. Connect the wires of the keypad to the terminals of the PassPoint MLB as per the table below.**

| Keypad Wire       | MLB Terminal |
|-------------------|--------------|
| Red (+12VDC)      | 11           |
| Black (Ground)    | 12           |
| Green (Data In)   | 13           |
| Yellow (Data Out) | 14           |

- 6. Re-attach the keypad to its case back.**

## **Setting the keypad address**

The keypad's address must be set to "00" in order for it to function properly. If the address is not set correctly, an error message will appear on the keypad display when the PassPoint system is powered up. To set the keypad address:

### **1. Power up the PassPoint system.**

The keypad must be powered-up in order to set the address. Powering up the PassPoint system powers up the keypad.

To power-up the system, plug in the system's wallpack transformer.



---

Do not attempt to power-up the system/keypad until previously described connections have been made.

---

### **2. Within 60 seconds of power-up, press and hold down the "1" and "3" keys of the keypad simultaneously.**

Pressing and holding down these keys puts the keypad into address mode. The current keypad address will be shown on the display ("31," the default address).

### **3. Press the "0" key twice to enter the new address, then press the star "\*" key.**

Pressing the star key saves the new address.

Once the proper address of "00" has been entered, the keypad will display the name of the system, the date and the time (all of which are user-configurable).



---

## ***Where do you go from here?***

Now that all of your system hardware has been wired and mounted, you are ready to install the PassPoint *Express* software. This software will enable you to configure and operate the PassPoint system.

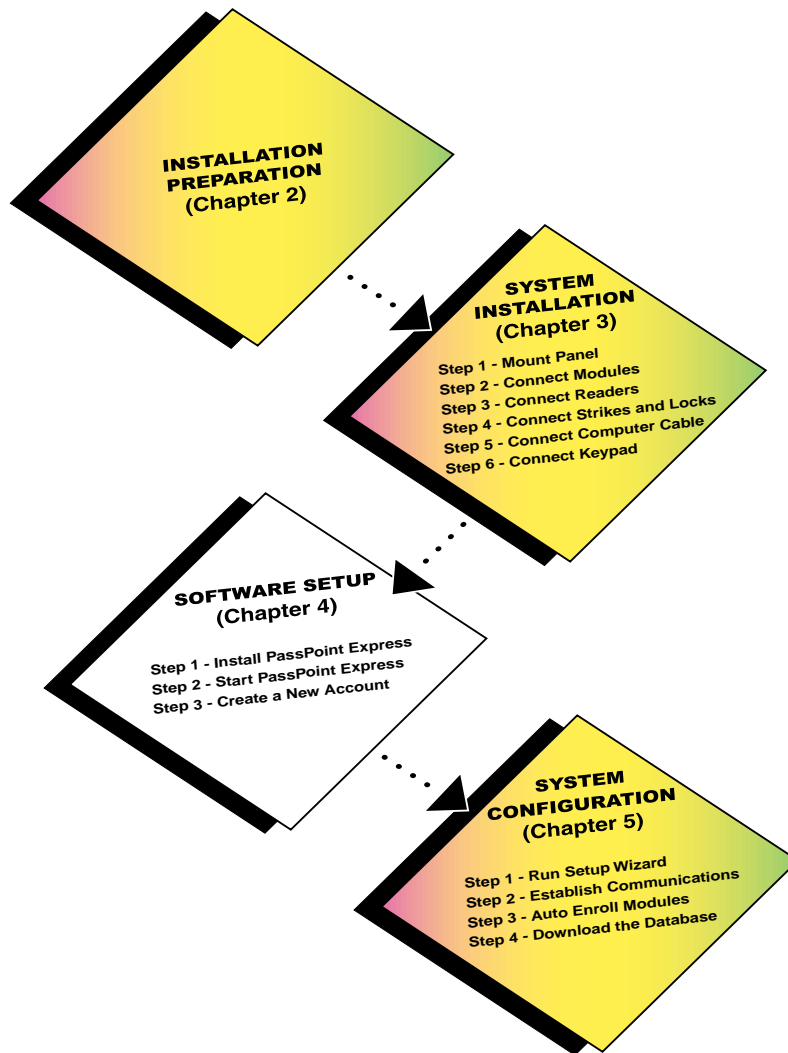
Chapter

# 4

## *Software Setup*

This chapter explains the basic use of the PassPoint *Express* Windows software program. In this chapter you will learn:

- **What PassPoint *Express* is and what its system requirements are**
- **How to install PassPoint *Express* on your user terminals**
- **How to start PassPoint *Express***
- **How to log on to PassPoint *Express***
- **How to set up the communications parameters for PassPoint *Express***





**STEP 1**  
**Install**  
**PassPoint Express**

The first step in software setup is to install the PassPoint *Express* software on your user interface (i.e., PC). Refer to the section of this chapter titled '*Step 1 - Install PassPoint Express*' for instructions on performing this step.



**STEP 2**  
**Start**  
**PassPoint Express**

Once the PassPoint software is installed, you can start it up. Refer to the section of this chapter titled '*Step 2 - Start PassPoint Express*' for instructions on performing this step.



**STEP 3**  
**Create a**  
**New Account**

The first thing you must do after starting PassPoint *Express* is set up your Account. Each MLB in your system will have one Account. Accounts let you manage multiple MLBs. Refer to the section of this chapter titled '*Step 3 - Create a New Account*' for instructions on performing this step.

## ***What Is PassPoint Express?***

PassPoint Express is a Windows 95 software program that allows you to configure and operate the PassPoint access control system. Essentially, PassPoint *Express* allows your PC to communicate with the main logic board of the system.

With PassPoint *Express*, you can configure all of the options necessary to get your system up and running, perform system maintenance, and monitor system functioning. While monitoring the system, PassPoint *Express* displays a scrolling list of system events. A user can then log on and enter the program's visually oriented system, which allows full screen editing of configurable options.



---

The PassPoint system does not need to be connected to the PassPoint *Express* PC in order to function. The PC is only used to configure and monitor the system. Once the system is up and running, the PC can be disconnected (either intentionally or unintentionally) without disrupting the operation of the system.

---

## ***System requirements***

In order to install and run *PassPoint Express*, your PC will need to have the following minimum configuration:

### **Minimum**

- **P90 Class processor**
- **16 megabytes RAM**
- **20MB free hard disk space**
- **Windows 95 (not Windows NT)**
- **SVGA video display, 800x600 resolution, 256 color**
- **Mouse**
- **1 available serial port for MLB connection**

### **Optional**

- **1 available serial port for TWAIN digital camera (optional)**
- **TWAIN compliant scanner (optional)**
- **2 Hayes-compatible 28.8 modems (optional for remote operation)**
- **Integral Flashpoint Lite or better (optional for on-screen video)**

## ***Step 1 - Install PassPoint Express***

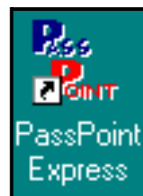
To install PassPoint *Express* on your PC, follow the procedure below:

- 1. Starting from the Windows 95 main screen, insert disk 1 from the set of disks supplied with your Access Starter Kit.**
- 2. In the Windows 95 Start Menu, select *Run*. In the dialog box that appears, type “a:/setup” and press *Enter*.**

In a few moments the first screen of the PassPoint *Express* installation program appears.

The PassPoint *Express* installation program has been designed to walk you step by step through the installation process. The program will prompt you for the necessary information. Each time you complete a step, click *Next* to go on to the next step.

Once you have completed the installation process, the PassPoint *Express* icon will automatically appear on your desktop and *Start* menu.

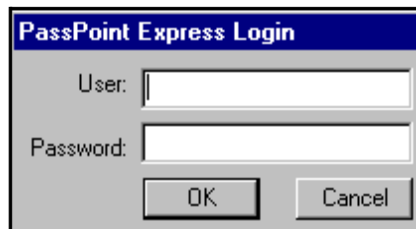


## Step 2 - Start PassPoint Express

To start PassPoint Express on your PC:

1. Select *PassPoint Express* from the Windows 95 Program menu.

In a few moments, the system will prompt you for a user name and password:

A screenshot of a Windows-style dialog box titled "PassPoint Express Login". It features a blue title bar. Below the title bar, there are two text input fields: "User:" and "Password:". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

2. Enter your default user name and password and click *OK*.



---

Both the default User name and Password are *installer*.

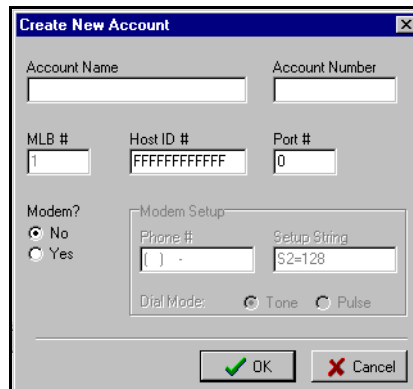
---

Once you click *OK*, the system brings up a new Account dialog box. In order to continue, you must create a new Account (see the next step in this chapter).

---

## Step 3 - Create a New Account

The first time you start PassPoint *Express*, the system prompts you with a dialog box for creating a new Account:



Before you can proceed to configuring your system, you *must* create a new Account.

### **What is an Account?**

In order to make using your system's database efficient, PassPoint uses system *Accounts*. An Account is a *partition* of a database that allows Express to manage more than one system (i.e. more than one MLB). Each MLB is assigned a specific Account number. Then, when you want to access a database (for backing up, event viewing, etc.), you select the applicable Account number.

Accounts help you manage the PassPoint system by treating each MLB as an independent unit. Each MLB is assigned a unique Account number. Using this number, you can back up and restore the database for a specific MLB, view the event log for the MLB, generate reports, etc. For installers who use PassPoint *Express* to administer multiple sites belonging to the same customer, a separate Account should be set up for each

site. This way, when you bring up PassPoint *Express*, you can select the Account (i.e., site) you want to work with.

Even though your Access Starter Kit has only one MLB, you still need an Account, because you cannot back up or restore the database without an Account. In this case, you will need to set up only one Account.

If the system is configured to dial into an alarm company central station, this Account number will be used to indentify all transmissions to the central station.

**What information is in the Account database?**

Each Account database entry stores the configuration information for the equipment installed at that site. This includes hardware configuration, schedules, Access Groups, and all of the card database information. Essentially, this is all the information necessary to replicate the site's programming on a new MLB, should the first system become damaged.

The first step is to create a new Account for the one MLB included with your Access Starter Kit. To do so:

**1. Fill in the fields of the dialog box.**

The fields of the dialog box are described below:

**Account Name** - This is the name of the Account for the MLB. You should provide the Account with an easy to remember name that describes it properly. For example, if this is Account for the main MLB of the system, you might name the Account "Main."

**Account Number** - This is the Account number associated with the MLB Account. This number can be up to four digits. Also, this number must correspond to the first four digits of the *Primary Subscriber Account Number* assigned to

the MLB.

**MLB Number** - This is the number of the Account's Main Logic Board. This number can be up to two digits. If you have only one MLB, this number should probably be 01.

**Host ID** - Enter the appropriate host ID number for this Account. The host ID will be used to fill in the appropriate field on the network/ID tab of the screen of the system wide options screen.

**Port #** - Select the communications port of the PC to which you have connected the PassPoint system. This can be COM 1, 2, 3, or 4.

**Modem?** - If you are using a modem to connect to the system, select *Yes*. If not, select *No*.



---

If your installation uses a modem, you will need to fill in the phone number at which your installed equipment can be reached. You may also need to modify the modem set-up string if your modem requires special operational functions.

---

**2. Click *OK*.**

Clicking *OK* creates the new Account. Once the Account is created, the system will present you with the Setup Wizard, a tool for configuring your system.

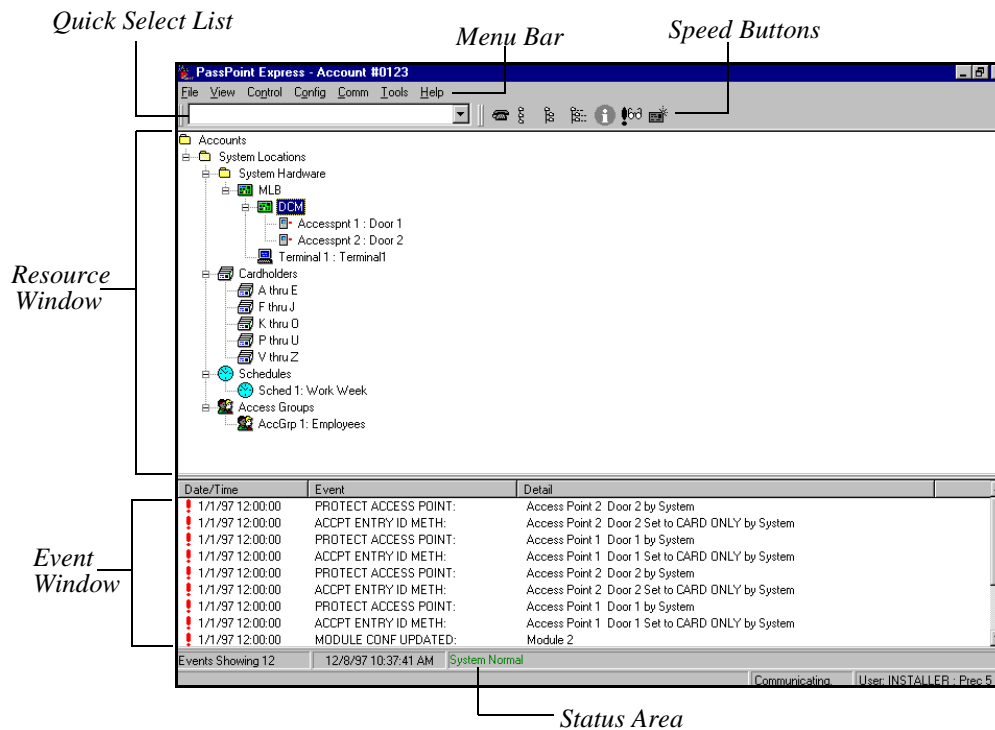
## ***The PassPoint Express Environment***

PassPoint *Express* has been designed to be simple to use. If you are already familiar with operating in a Windows environment, you should have no trouble finding your way around the PassPoint *Express* screen.



## Major screen components

The illustration below shows the main PassPoint *Express* screen as it would look if the system were fully up and running. This is, it includes card holders, time schedules, etc.



**Resource Window** - All of your system resources are listed in the Resource Window. Resources can be modules (like MLBs or DCMs), relays, zones, triggers, etc. Certain objects in the Resource Window can be controlled by right-clicking on them.

**Event Window** - Each time a new system event occurs, it appears in the Event Window. Examples of system events are bypassing a zone, enabling a relay, disabling a card reader, etc.

The most recent event appears at the top of the list in the Event Window.

**Menu Bar** - The menu bar allows you to select commands for the operation of the program.

**Quick Select List** - The Quick Select List lists all of your system's components and resources. Use the list to quickly locate the system objects you are looking for.

**Speed Button Bar** - Like the menu bar, the speed button bar allows you to select commands for program operation. Each speed-button function has a corresponding menu command on the menu bar.

**Status Area** - The Status Area provides information about the current operating conditions of your PassPoint system. Whenever an important system event or trouble occurs, a message indicating the event will appear here in red. In the illustration on the previous page, we can see that three important system events are in progress: a system module is failing communication, an Access Point is locked, and a zone is bypassed.

Chapter

5

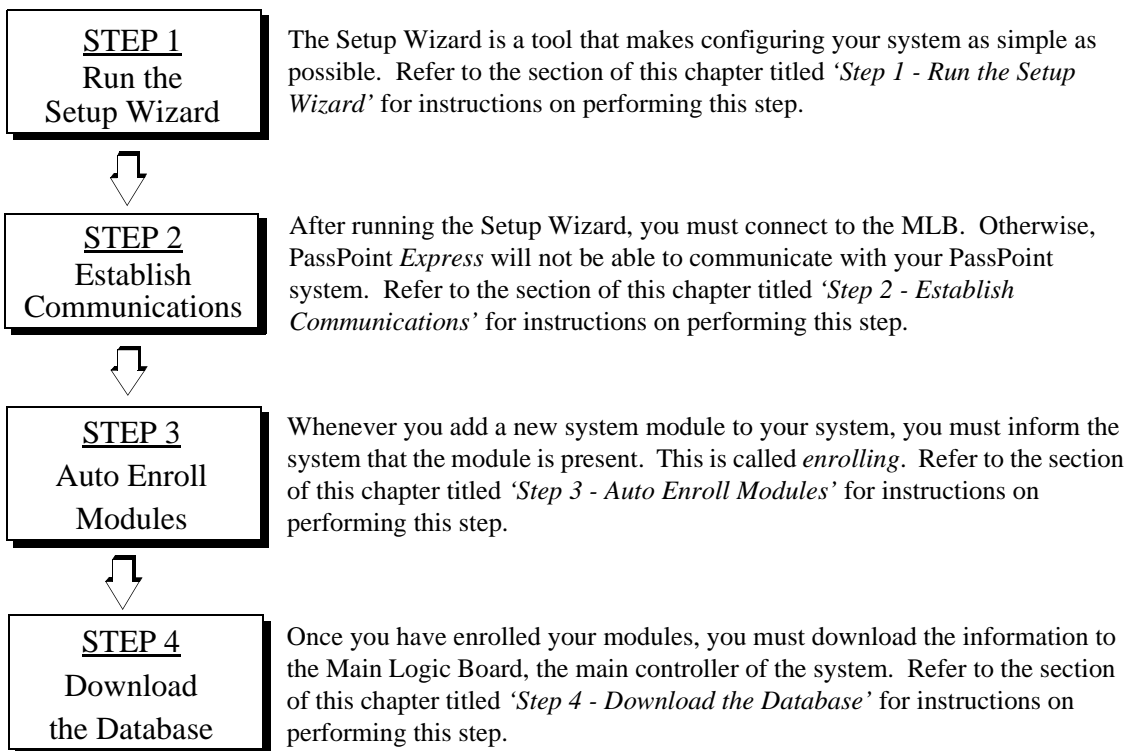
# *System Configuration*

This chapter explains the three main steps that need to be performed in order to get your PassPoint system up and running to a level that allows the first cards to be used.

In this chapter you will learn how to:

- **Set up your Access Points**
- **Enroll your system's Door Control Module**
- **Download the system database**
- **Enroll test cards and test the system**





---

## ***Step 1 - Run the Setup Wizard***

The first step in configuring your system is to run the Setup Wizard. The Wizard will help you to quickly set up your system by allowing you to choose from a predefined set of templates. Once you are done running the Wizard, your system will automatically have two doors, as well as a default Access Group, Day Template and schedule.

To use the Setup Wizard, simply follow the prompts on the screen. The first screen of the Wizard should already be on your screen:



This is the introductory screen. It explains a little of what the Wizard will do for you.

**1. Click Next.**

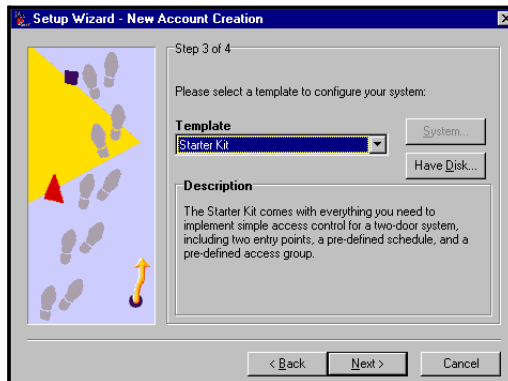
The second Wizard screen appears:



This screen presents you with three different setup options. The first option is the fullest option. It will configure your system, enroll your system modules, and download these settings to the database. Since you are setting up the system for the first time, this is the setup option to choose.

**2. Choose the first setup option, then click Next.**

The next screen of the Wizard appears:



This screen contains a drop-down list box that allows you to

select a configuration template. By default, the system displays Starter Kit as the template to configure. If you are only configuring a Starter Kit without an Expansion Kit or Card Enrollment Kit, select this option. Otherwise, select the appropriate option from the list. For the purposes of this discussion, we will assume you are only configuring a Starter Kit.

**3. Select a template, then click *Next*.**

If you have chosen the Starter Kit template, the final screen of the Wizard appears:



Click *Finish* in this screen to finish your configuration. The system will automatically create your two Access Points (i.e. doors), and create a default Access Group, Day Template and schedule. You will be learning how to use each of these items in later chapters of this guide.

Once the new account is configured, the system will prompt you to connect to the MLB so that you can enroll your modules and download the new configuration.



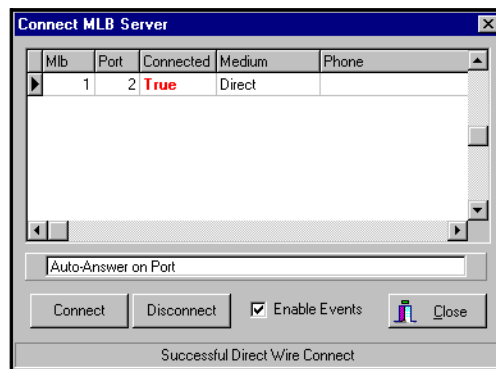
## Step 2 - Establish Communications

After running the Setup Wizard, you must connect to the MLB. Otherwise, PassPoint *Express* will not be able to communicate with your PassPoint system.

Before setting up PassPoint *Express*, make sure you have connected your PassPoint system to your PC. A null modem cable has been provided for connecting the RS-232 connector of your MLB to one of the COM ports of your PC. If you do not have this cable, you must use a null modem cable instead.

Power up the panel and wait for the keypad to display the message “LOCAL ONLINE.” If you are using a modem at the panel, press and release \* # , then wait for the keypad to display the message “REMOTE OFFLINE.”

The Connect to MLB dialog box appears immediately after running the Setup Wizard:



This dialog box displays information about your MLB connection parameters.

**1. Click *Connect*.**

After a few moments, the *Connected* field will change from “False” to “True,” indicating that connection has been established between your PC and your system’s MLB.

If you have chosen a modem connection, the modem connected to the PC will dial the appropriate phone number in order to reach the “remote” MLB.

**2. Click *Close*.**

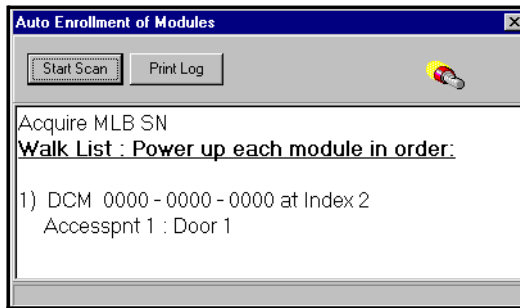
The MLB has now established a connection with the PC.

## ***Step 3 - Auto Enroll Modules***

After connecting to the MLB, the system will automatically prompt you to enroll your modules. Whenever a new module is added to the system, it must be enrolled. Enrolling simply informs the system database that a new system module is present.

When you enroll a system module, the system goes out and searches for any modules connected to it that have not been enrolled. Your kit template defines the hardware modules that the system expects to find. It knows which modules are not enrolled because these modules have serial numbers that begin with 0000. For instance, look at the DCM you have just added with the Wizard. It has a serial number that begins with 0000. That means that it has not been enrolled, and that it is not truly part of the system yet:

The Auto Enroll dialog box should already be on your screen, and should look something like this:



As you can see, the dialog box contains instructions. First, the system will acquire the serial number for the MLB. Then it will scan for the DCM and enroll that serial number as well.

This is all done **automatically** once you click *Start Scan*. The entire process will not take more than a few moments. The system knows which modules to look for because of the Starter Kit template you chose using the Setup Wizard. If you had chosen a different template, say a Starter Kit with a Card Expansion Kit, the system would also scan for a CPM.

**1. Click the *Start Scan* button.**

The system will go out and search for the modules. When it finds them, it will blink the yellow service LED on each module and present a screen message saying when each module has been enrolled.

The system will stop scanning for modules. If you had been enrolling more than one module, you would have had to wait until the system told you that all the modules had been enrolled.

**The Print Log button**



AutoEnroll dialog box contains a Print Log button that automatically prints a “walk list” of all the modules waiting to be enrolled.

You must power-up the modules in the order in which they appear in the walk list. Be certain the subsequent modules are powered-down when you begin the enrollment process. Once you start the scan and properly enroll each module, you may leave the module powered-up.



---

Never power-down the MLB during this process.

---

## **Step 4 - Download the Database**

The last step to getting your system operational is to download the database.

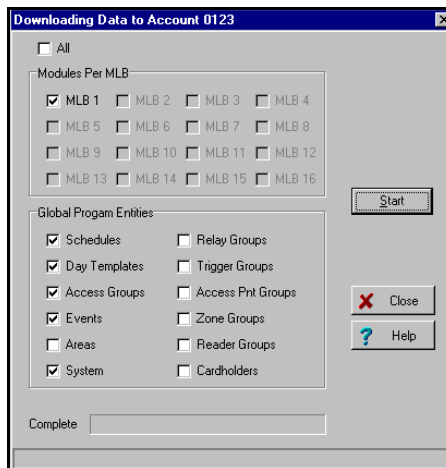
The PassPoint system database resides on the MLB. Here is where all of your system configuration data is stored. However, when you make changes on your PC, these changes are not automatically made to the database on the MLB. They are kept in a temporary storage area on your PC until you download them to your MLB database. Any changes made on the PC must be downloaded to the database in order for them to take effect.

*For example, you have already added a DCM to the system. The DCM has one or two doors that you have configured. This information is all displayed in the PassPoint Express window. It resides in the PC database. But it does not yet reside in the primary MLB database, because you have not downloaded it yet.*

To download the database, follow the procedure below:

**1. From the *Config* menu, select *Download*.**

The Download dialog box appears:



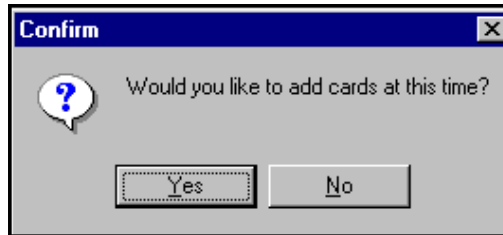
At the top of the dialog box is the account number you will be downloading. There are also checkboxes in the dialog box that tell you what information you will be downloading. These checkboxes are automatically checked according to the kit template you have selected.

**2. Click *Start*.**

The database download will proceed. The status bar at the bottom of the dialog box will track the progress of the

download.

When download is complete, a dialog box will appear asking if you want to add cards.



Clicking *Yes* automatically launches the Card Wizard, a PassPoint tool used for quickly adding cards to the system.



---

Adding cards to the system is covered fully in the next chapter of this guide.

---

Chapter

# 6

## *Managing Cards and the Cardholder Database*

In this chapter you will learn how to:

- **Use the Cardholder database**
- **Use the Card Wizard to add a single card or a batch of cards**
- **Add a card to the database manually**
- **Associate an action with a card**

---

## About the Cardholder Database

In order to keep track of all of its Cardholders, PassPoint uses a database. The PassPoint Cardholder database contains the names of all of the Cardholders of the premises. It associates each Cardholder with his/her ID card's code, as well as the Cardholder's Personal Identification Number (PIN). It is here, in the Cardholder database, that you assign cards and PINs to Cardholders.

### ***Adding Cardholders to the system***

Each time you want to issue a card, you are adding a Cardholder to the database. In addition to the Cardholder's name, ID card and PIN, you can enter such information as the Cardholder's Access Group assignments, the type of card he/she is using, etc. Some of this information is mandatory to enter. Other information is optional and is intended to make locating and managing Cardholders easier.

*For example, Cardholders can be assigned to up to five different Access Groups, but they must be assigned to at least one. Otherwise, they will never be able to access any of your premises' Access Points.*

Also, each Cardholder card can be assigned to invoke a specific system action. The action can be set to initiate under a variety of circumstances, such as an access grant, an access denial, or an egress grant.

Cards can be assigned to Cardholders on a temporary basis, allowing an expiration date or usage count to determine the period throughout which the card will be valid.



*For example, if you want to give a card to a visitor for only one day, you can set the card to expire on the following day. Or, if you want the card to only work for three entries into your building, you can set the card to deny every entry request after the third.*

**Where do you start?**

In Chapter 5, you configured your system and were prompted to add cards. Essentially, adding cards is the last step in the setup process. The system prompted you with the Card Wizard, as shown below:



You can also call up the Card Wizard by clicking the Add Card button on the button bar.

There are two main ways to enroll a card. One is to use the Card Wizard. The other is to use the *Add New Card* function. Both methods are explained below:

- **The *Add New Card* function**

This function is chosen from the *Config* menu, and brings up a dialog box that allows you to fill in the data for the card manually.

Adding a card with the *Add New Card* function allows you the greatest flexibility. The Card dialog box contains a number of fields that can be edited and tailored for the particular Cardholder.

The *Add New Card* function allows you to add only one card. If you want to add more than one card, use the Card Wizard.

- **The Card Wizard**

The Card Wizard is a PassPoint tool that lets you enroll cards quickly and easily. Using the Card Wizard, you can enroll a single card, or you can enroll a batch of cards.

Adding a card using the Card Wizard only allows you to add basic, default information to the card. It does not allow you the flexibility that adding a card manually does. However, once you have added a card using the Card Wizard, you can go back and add more specific information to that card.

## ***Using the Card Wizard***

The quickest and easiest way to add cards is to use the Card Wizard. With the Card Wizard, you can add one card or a batch of cards.

The Card Wizard appears automatically as the last step of the configuration process:



The Card Wizard works in the same manner as the Setup Wizard (shown earlier in this guide). To use the Card Wizard, simply follow the instructions and answer the prompts.

**3. Click *Next*.**

The first step is to determine whether you want to add one card or a batch of cards. Make your selection by choosing the appropriate option:

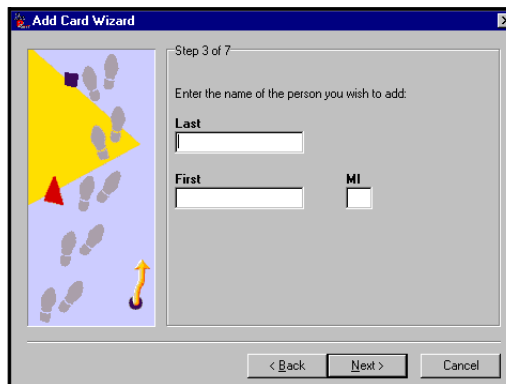


## ***Adding a single card***

To enter a single card using the Card Wizard:

**1. Select *Add a single card* in the Wizard and click *Next*.**

The Wizard will ask you to enter a last and first name for the Cardholder (i.e., the person to whom the card will be assigned):



**Add Card Wizard** Step 3 of 7

Enter the name of the person you wish to add.

**Last**

**First** **MI**

< Back Next > Cancel

**2. Enter the appropriate name information into the fields and click *Next*.**

The system will prompt you to enter card information:



**Add Card Wizard** Step 4 of 7

Please present the card to the enrollment reader now, or if you prefer, enter in the information below.

Note: You may enter either the card number (hot stamp) from the back of the card, or, if the card calculator is set to *Flaw Card Image*, you may enter the actual card code.

When entering a card number, the card code will be computed automatically based on the current card calculator settings.

Current Card Calculator Setting: [34 Bit ADEMCO Prox NCC](#)

To change the card calculator settings, click here: 

**Card Number** **Card Code**

< Back Next > Cancel

If you have a Card Enrollment Kit, you can swipe the card at your enrollment reader to enter the card information. Otherwise, key the applicable card information into the screen manually.



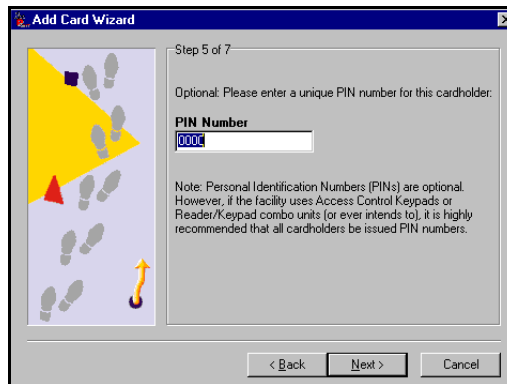
---

The default card setting is 34-bit Ademco proximity.

---

**3. Enter the card information and click *Next*.**

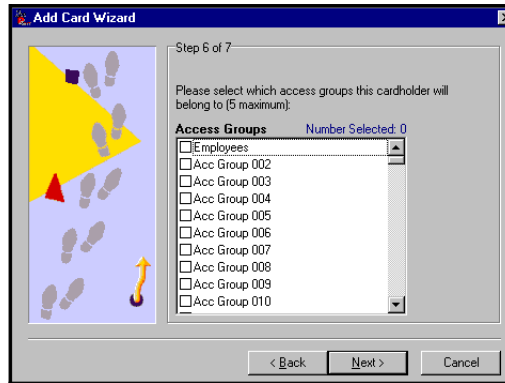
The Wizard will ask you to enter a PIN number for the card. This is an optional step and only needs to be done if your system uses keypad readers that enable a PIN to be used:



**4. Enter a PIN number (if applicable) and click *Next*.**

Next, the Wizard will ask you to choose Access Groups for

the card:



Each Cardholder can be assigned to up five Access Groups. To assign an Access Group to a user, simply check the number of the group(s) in the boxes provided.



---

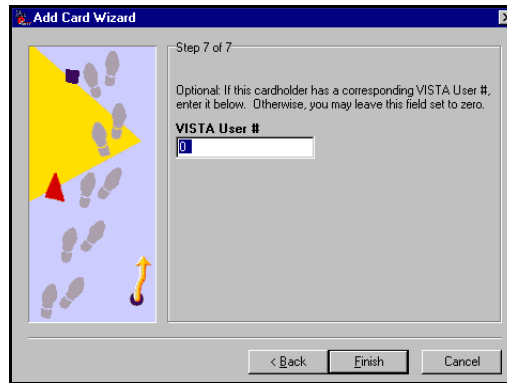
The ASK template includes one pre-set Access Group, called EMPLOYEES. This enables you to choose an Access Group without first having to create one. Later, you can modify or delete the EMPLOYEES Access Group if you want.

---

In order for a Cardholder to have any access privileges at all, he/she must be assigned to at least one Access Group (unless the Cardholder has been granted executive privileges).

**5. Select the Access Groups for the card, then click *Next*.**

The last step is to enter a Vista user number (if applicable):



If the Cardholder has a corresponding Vista user number, enter it in the field provided. If not, leave this field blank.

**6. Click *Finish*.**

The card will be added to the Cardholder database. From here you can view, edit, or delete the card.

***Adding a batch of cards***

There are two ways to add a batch of cards: batch add and batch swipe.

**Batch Add**

Batch adding allows you to quickly add a batch of cards at one time. The Card Wizard will ask you to swipe (or manually enter) the FIRST and LAST card in a batch. The cards must be in numerical order for this method to work. Once this is done, PassPoint will automatically enroll both the first and last card, and every card in between.

Using this method does not allow you to enter Cardholder names for the cards. This must be done separately for each card, along with any other specific card information you want to add.

### **Batch Swipe**

The batch swipe method also allows you to add a batch of cards, but this method requires you to swipe each card one by one at a card enrollment reader.

Once the cards have been swiped, you then choose an Access Group for the cards. Also, this method gives you an option of entering a Cardholder name for each card you enroll.

## ***Adding Cards Manually***

If you don't want to use the Card Wizard to add a Cardholder to the database, you can simply add the card manually. Adding a card manually allows you greater flexibility when adding cards, since there are many more information fields available to you that allow you to customize the card.

To manually add a card, follow the procedure below:

- 1. From the *Config* menu, select *Cards>Add New Card*.**



The Card Data dialog box appears:

*Each tab allows you to add/edit different data for the card.*

*Use the Card Data dialog box to add new cards, edit card data, and delete cards.*

The Card Data dialog box allows you to enter various types of information about each card. Each tab of the box displays a different set of data. When creating a new card record, you fill out these fields as applicable. Some of these fields, like *Last Name* and *Access Groups*, are mandatory. Others need not be filled, or already contain default data that can be used. The fields that you choose to fill out for each card will depend upon the Cardholder, the needs of the installation, and other factors specific to the premises.

## 2. Fill out the fields of the first tab, *Access*.

The first tab of the Card Data dialog box is the only tab that contains fields that must be filled in for the card to function. Each of these tab fields is explained below:

**Name (Last, First, MI)** - Enter the name of the Cardholder

in these three fields. The name does not have to be unique, and the manner in which the name is capitalized is not important.

**Card #** - Enter the card number in this field. The card number entered will automatically compute the correct *Card Code*, provided that the proper *Card Technology* has been chosen.

**Card Technology** - In this field, select the proper card technology type that your system is using.

---



This field must be filled in correctly in order for the card to function. By default, this field will read “34 Bit Ademco Prox NCC,” which is the type of card shipped with the Access Starter Kit.

---

**Card Code** - The card code is the actual code embedded in the card. This is the code that the system reads when the card is presented to a reader. This field cannot be edited. It updates automatically according to the *Card #* entered and the *Card Technology* chosen in the two previous fields.

**PIN Code** - In this field enter the 8-digit personal identification number (PIN) that you want to assign to the Cardholder.

Personal Identification Numbers can be 3 to 8 digits long. A system option sets the PIN code length that is used throughout the system. All PIN codes in the system must be unique to a length of 1 digit less than the system PIN length. In other words, if the system PIN code length is set at 4 digits, the first 3 digits of ALL of the PIN codes in the system MUST be unique. The last PIN digit is a “don't care” — any PIN digit can be assigned in this position. However, never

define a PIN code that ends in “0.” This is because any PIN code typed in at an Access Point that ends in “0” may be interpreted as an access request under duress. It might be wise to assign PIN codes that all end in the same digit — for instance, “9.” This is because other special “last” digits may be used by future versions of the system. Note that if a card ID is not entered for this Cardholder (as might be the case of PIN-only systems), data **MUST** be entered in this field.

**Access Groups** - In the list boxes provided, select up to five Access Groups for the card.

In order for a Cardholder to have any access privileges at all, he/she must be assigned to at least one Access Group (unless the Cardholder has been granted executive privileges, as explained above).

**Disabled** - If you should want to disable the privileges of the Cardholder, check this box. While disabled, all of the Cardholder’s access privileges will be revoked. You can reinstate the Cardholder’s privileges at any time by unchecking this box. While disabled, the card will remain in the system database. When disabling a card, enter a date that tells the system when to disable the card.

**Use Expiration Date** - If you want the card to become invalid after a specific date, check this box and enter the date in the field provided. Any attempted use of the card after this date will be denied.

**Use Expiration Count** - If you want the card to become invalid after a specific number of uses, check this box and enter the number of valid uses in the field provided. For example, enter “10” in this field if you want the card to allow only ten access grants.

**Refresh Count** - Click this button to refresh expiration count from MLB.

**Vista User #** - If there is a Vista control panel user number associated with the Cardholder, enter the applicable number in this field.

**Executive Privileges?** - Check this box if you want to grant the Cardholder executive privileges: full access to all of the system Access Points. The Access Groups assigned to the Cardholder will not be checked, so it is not strictly necessary to assign any Access Groups to the reader (although it is highly advisable, since executive privileges are revoked whenever the system is in Threat Level 5).

Note that enabling this field may have security ramifications that must be managed by the system's administrator. Also, if threat levels are used by the facility, any Executive Privilege card should also be assigned at least one Access Group. The Access Group assigned **MUST** be valid during Threat Level 5 so the person will have an escape path from the premises. Not providing such an escape path can have life and safety implications. Executive Privilege cards also retain all the access privileges of all Cardholder Authority Levels.

**Trace?** - Check this box if you want to log a trace event each time the card/PIN code is used. A trace event appears in the event log of the system and "traces" the movements and actions of the Cardholder. Generally, this field will not be used unless a card needs to be "watched" for some reason.

**3. Fill in the fields of the remaining tabs, or click *Save*.**

At any point after filling in the first tab fields, you can save the card record and add the card to the database.

The remaining tabs of the dialog box allow you to enter additional information for the Cardholder. For example, the *Personal* tab allows you to add personal data about the Cardholder, such as his/her address. The *Summary* tab allows you to view summary information about the Cardholder at a glance.

### Using the Custom tab

The *Custom* tab contains user-configurable fields that can include any pertinent information you wish. When you first open the *Custom* tab, it's essentially blank. This is because no fields have been configured yet.

To configure fields for the *Custom* tab:

1. From the *Config* menu, select *Cards>Options*.

The Card Data Configuration dialog box appears:

| Enable Field                        | Vis. Ver. Form           | Field Name             | Field Description |
|-------------------------------------|--------------------------|------------------------|-------------------|
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Enter Custom Name Here |                   |
| <input type="checkbox"/>            | <input type="checkbox"/> |                        |                   |
| <input type="checkbox"/>            | <input type="checkbox"/> |                        |                   |
| <input type="checkbox"/>            | <input type="checkbox"/> |                        |                   |
| <input type="checkbox"/>            | <input type="checkbox"/> |                        |                   |
| <input type="checkbox"/>            | <input type="checkbox"/> |                        |                   |
| <input type="checkbox"/>            | <input type="checkbox"/> |                        |                   |
| <input type="checkbox"/>            | <input type="checkbox"/> |                        |                   |

This dialog box contains various fields that let you customize the *Custom* tab.

**2. Check off the boxes of the fields you want enabled.**

**Enable Field** - This will allow users to type into these fields in the *Custom* tab of the Card Data dialog box.

**Vis. Ver. Form** - Check this box if you want the field displayed on the Visual Verification dialog box.

**Field Name** - In this field, enter the text to be used as the title of the field in the *Custom* tab.

**Field Description** - In this field, enter the text to be used as the help text for the field in the *Custom* tab.

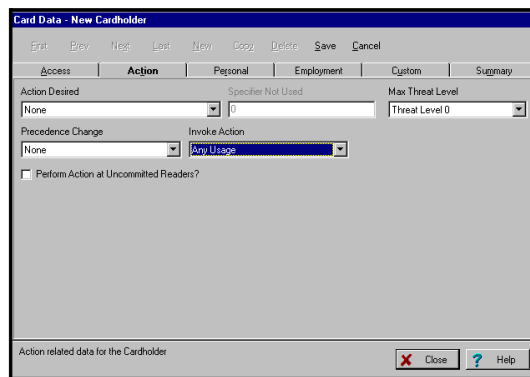
**3. Click OK.**

The system will automatically update the information for the *Custom* tab. Next time you open the Card Data dialog box, the *Custom* tab will reflect the data you just entered.

## ***Using the Action tab***

You can configure the system to perform a specific action whenever a specified event occurred with the card (such as an access grant). To do so, use the fields of the Action tab:

*Use the Action tab to associate an action with the use of the card.*



**Action Desired** - This is the function you want to occur when the card is used. Make your selection from the predefined list of actions.

**Specifier** - This is the system item acted upon. For instance, if you've chosen "Relay On" as your action, the specifier would be the relay number.

**Maximum Threat Level** - This is the threat level at which the action will be allowed to take place. If the system threat level goes beyond the setting for the action, the action will not be allowed to occur. The default value for this field is 0, meaning normal.

**Precedence Change** - This field indicates how the precedence level of the Specifier (above) will be affected when the action takes place. You can choose None, Clear the precedence level to 0, or Update to have the resource take on the precedence level of the Cardholder

**Invoke Action** - In this field, select the specific system occurrence upon which you want the action to occur. The action will only take place when the card encounters the situation specified in this field. For instance, you can select the action to occur when an access request is granted. Or you can select the action to occur when an access request is denied.

**Perform Action at Uncommitted Readers?** - Check this box if you want the action specified to occur when the card is used at an uncommitted command reader.





## *Section Two*

---

•

## *Expanding PassPoint*



Chapter

# 7

## *Adding a Door Expansion Kit*

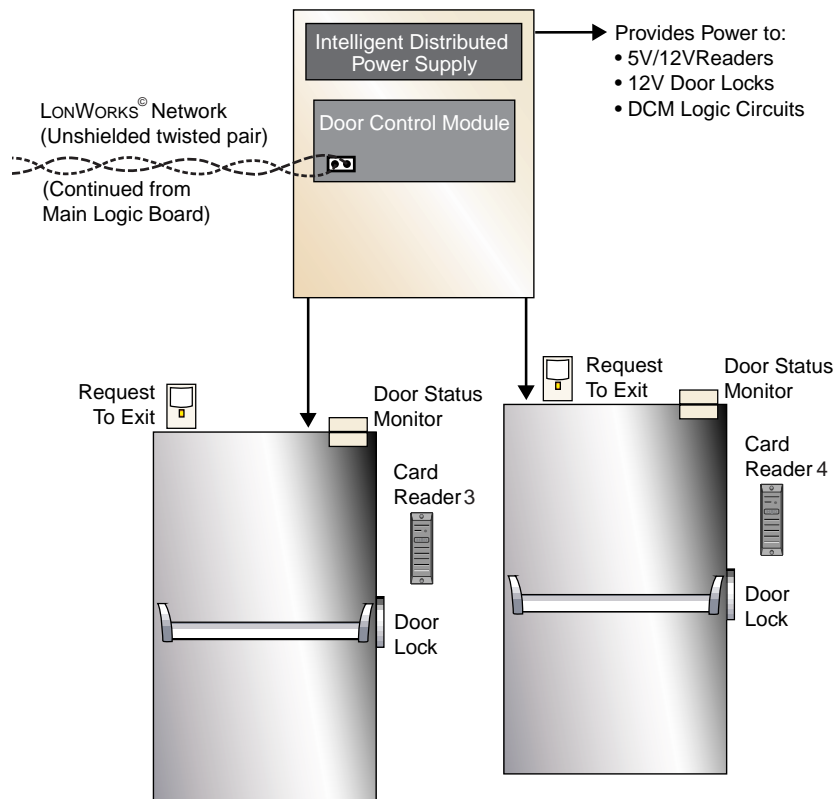
Adding a Door Expansion Kit (DEK) allows you to quickly add two more Access Points to an existing PassPoint installation.

In this chapter you will learn how to:

- **Mount the DEK control panel**
- **Wire all of the components of the DEK**
- **Activate and set up the DEK**
- **Enroll the DEK into an existing PassPoint system**

## Understanding Your Door Expansion Kit

The PassPoint Door Expansion Kit allows you to quickly add two more doors to your existing PassPoint installation. Essentially, the DEK consists of a Door Control Module and power supply, mounted in a standard cabinet. Once the DEK is connected to your existing system, you need only to enroll the new Door Control Module and set up your new Access Points.



**DOOR EXPANSION KIT (DEK)**

***What's in your  
Door Expansion  
Kit?***

Your PassPoint DEK consists of the following hardware components:

- **1 pre-configured access panel, consisting of the following:**
  - 1 metal enclosure
  - 1 Door Control Module
  - 1 power supply
- **1 plug-in transformer**

## ***Installing the DEK***

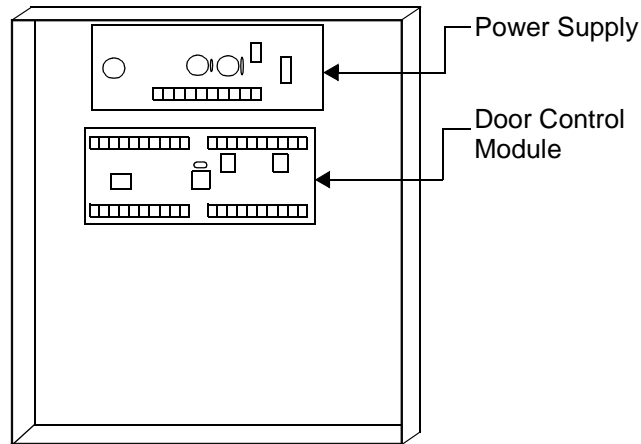
There are six simple steps that must be completed in order to install and enroll the DEK into an existing PassPoint system. Follow each of the steps below and follow the wiring diagram provided.

### ***Step 1 - Mount the DEK panel***

The DEK panel (or cabinet) contains the kit's Door Control Module and power supply.

When the door to the panel is removed, the inside of the cabinet looks like this:

*DEK Panel with DCM and power supply.*



### **Choosing a mounting area**

When selecting a mounting area for the panel, choose a clean, dry place not readily accessible to the general public but convenient enough so that a technician can get at the panel easily. The panel should be mounted on a sturdy wall using fasteners or anchors (not supplied in your kit).

- 1. Position the cabinet on the wall and use the holes in the back of the cabinet to mark your four mounting holes.**
- 2. Using four anchors or fasteners, mount the cabinet to the wall.**



---

When mounting the cabinet, be very careful not to jar the system's PC boards. Also, be careful not to accidentally pull off any of the wires connecting the modules. If any of the wires do come loose, re-connect them according to the Summary of Connections diagram.

---

## Step 2 - Connect the DCM

Connecting the DCM actually involves three steps:

- **Connecting the DCM to the power supply and system's MLB**
- **Connecting the power transformer**
- **Connecting card readers**



---

When making these connections, refer to Appendix A, Wiring Considerations, for additional diagrams and system ratings.

---

### **Connecting the DCM to the MLB and power supply**

1. **Connect the *local* power jumper between power supply connector J5 and DCM connector J1.**
2. **Connect two network connection leads between the MLB and DCM.**

Connect one lead between terminal 1 of the DCM and terminal 16 of the MLB.

Connect the other lead between terminal 2 of the DCM and terminal 15 of the MLB.

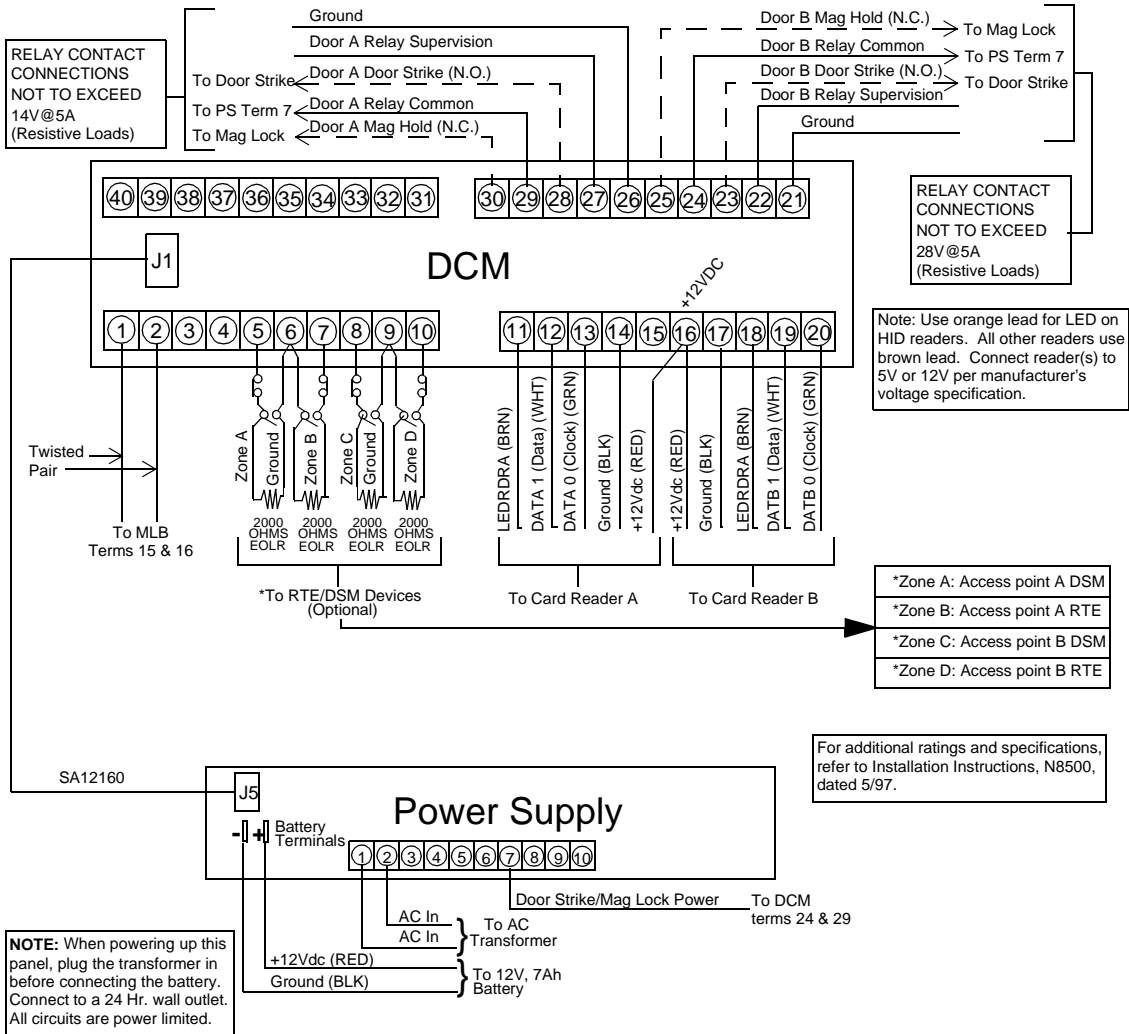
### **Connecting the power transformer**

The DEK comes with a wall pack power transformer that needs to be wired to the DCM. To do so:

**Connect the leads of the power transformer to terminals 1 & 2 of the DEK power supply.**

### **Connecting card readers**

Card readers are not included with the DEK and must be purchased separately. Refer to the documentation accompanying your card readers for proper installation instructions. If you have purchased PassPoint proximity readers, refer to the applicable section of this guide.



### Step 3 - Activate the system

Once the DCM has been connected and all door control hardware has been mounted and wired to the system, you can



activate the system. To do so, plug the power transformer into a suitable wall outlet. The wall outlet must be a 24-hour power source.

## Step 4 - Add and set up the DCM

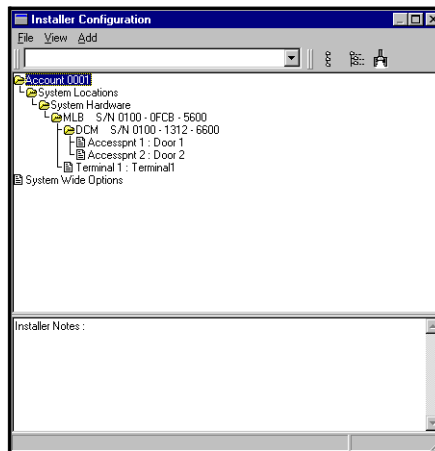
Now that the DEK is powered up, you must add the new DCM to your existing installation, and set up your doors. To do this, you will be using the Setup Wizard described in Section One of this guide.

To add and set up the new DCM, follow the procedure below:

### 1. From the *Config* menu, select *Hardware*.

The Installer Configuration dialog box appears:

*Use the Installer Configuration dialog box to view/modify system components and to set various system options.*



The Installer Configuration dialog box lists all of the components of the system. Here is where you add system modules such as DCMs. This dialog box is also used to set various system options, such as skeleton codes and modem

settings.

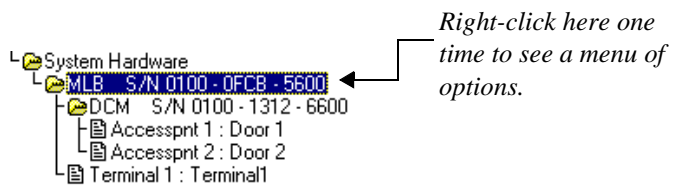


---

Once you make changes in this screen, the changes must be downloaded to the system database in order for them to take effect.

---

**2. Right-click on the MLB once.**



This will bring up a menu of options.

**3. From the menu, select *Add DCM*.**

The Setup Wizard appears:



**4. Click *Next* to continue.**

Clicking *Next* always brings you to the next screen of the Wizard:



**5. Specify how many Access Points you want to configure.**

The Wizard gives you three options:

- **One Entrance Point**
- **Two Entrance Points**
- **One Entrance/Exit Point**

The option you select will depend upon the needs of your installation. For the sake of this procedure, we will assume that we are only configuring one entry point. The procedure for configuring two Access Points is essentially the same.

When you have made your selection, click *Next* to continue.

**6. Enter the name of the Access Point.**

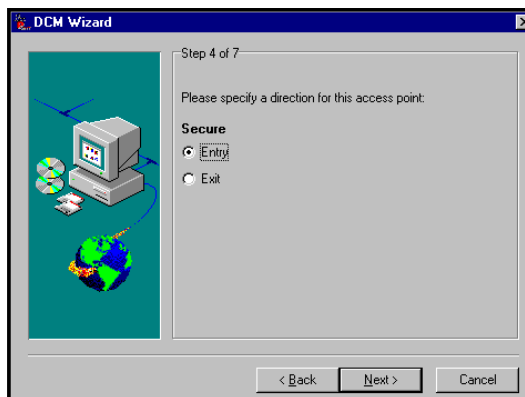
The name should be something descriptive of the door, e.g. “Front Door” or “Warehouse Door.”



Once you have entered a name for the Access Point(s), click *Next* to continue.

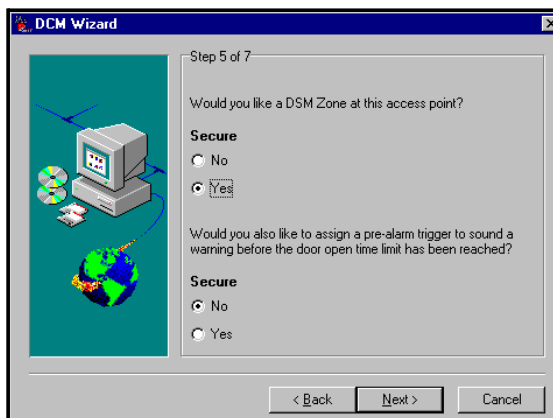
**7. Choose a direction for the Access Point.**

You can choose to make the Access Point either an entry point or an exit point:



After choosing a direction, click *Next*.

**8. Choose whether or not you want Door Status Monitoring (DSM) for the Access Point.**



DSM is a function that allows the system to monitor how long a door is kept open, and sounds an alarm if that amount of time is violated.

If you select to use DSM for a door (as shown in this example), the system will then ask you if you want to set a pre-alarm trigger for the door. The pre-alarm trigger is a warning signal that sounds before the door goes into alarm. It is used to warn individuals that the door will go into alarm if they do not close it immediately.

When you have made your DSM selections, click *Next* to continue.

**9. Choose whether or not you want Request-to-Exit (RTE) for the Access Point(s).**



An RTE zone is a device connected to the door that requires system verification before allowing a Cardholder to exit through the door. An RTE device may be a button for the Cardholder to push, or it may be a motion detector that detects when a person is coming toward the door to exit. When the device is pushed (in the case of the button) or senses a person (in the case of the motion detector), the system will unlock the door and allow the person to exit.

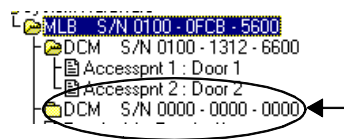
When you have made your RTE selection, click *Next* to continue.

The Wizard will present you with a summary screen of your Access Point configuration choices:



**10. Click *Finish* to exit out of the Wizard and save your changes.**

The tree in the Installer Configuration dialog box will now show your new DCM, along with any Access Points you configured using the Setup Wizard:



*Once you finish with the Wizard, your DCM and Access Points appear in the tree.*

Although you have configured your DCM and Access Points, you must still enroll the DCM so that the system recognizes it and all its configuration settings. Enrolling the DCM is covered in the next step.

---

## Step 5 - Auto enroll the DCM

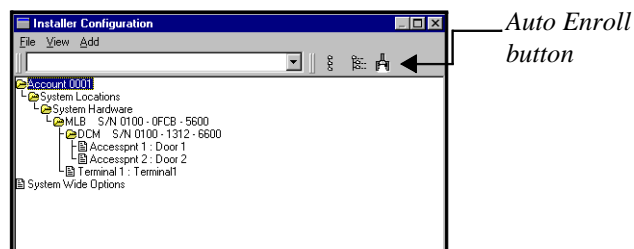
Whenever a new module is added to the system, it must be enrolled. Enrolling simply informs the system database that a new system module is present.

When you enroll a system module, the system goes out and searches for any modules connected to it that have not been enrolled. It knows which modules are not enrolled because these modules have serial numbers that begin with 0000. For instance, look at the DCM you have just added with the Wizard. It has a serial number that begins with 0000. That means it has not been enrolled, and is not truly part of the system yet.

To enroll the DCM you just configured, follow the procedure below:

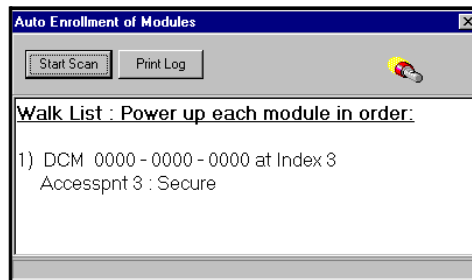
**1. Click the Auto Enroll button on the Installer Configuration dialog box.**

Refer to the diagram below for the location of the Auto Enroll button:





Clicking this button brings up the Auto Enroll dialog box, shown below:



The enrollment process is all done **automatically** once you click *Start Scan*. The entire process will not take more than a few moments.

**1. Click the *Start Scan* button.**

The system will go out and search for the DCM. When it finds it, it will blink the yellow service LED on the DCM and present a message saying when the DCM has been enrolled.

The system will stop scanning for modules. If you had been enrolling more than one module, you would have had to wait until the system told you that all the modules had been enrolled.

## ***Step 6 - Download the database***

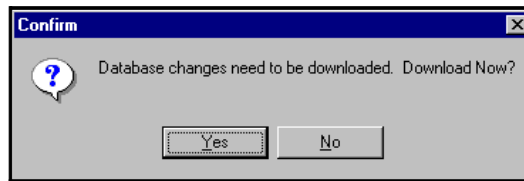
The last step to getting your DEK operational is to download the database.

Remember, the PassPoint system database resides on the MLB. Here is where all of your system configuration data is stored. However, when you make changes on your PC, these changes

are not automatically made to the database on the MLB. They are kept in a temporary storage area on your PC until you download them to your MLB database. Any changes made on the PC must be downloaded to the database in order for them to take effect.

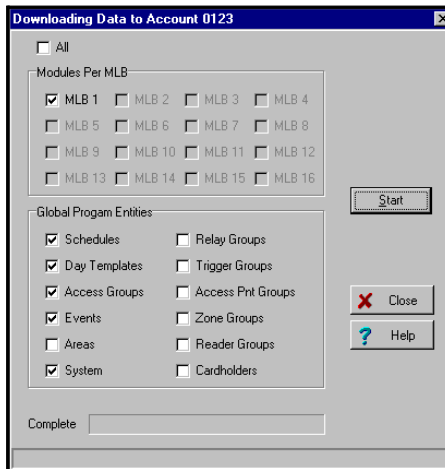
**1. Close the Installer Configuration dialog box.**

The system will automatically ask you if you want to download the database:



**2. Click Yes.**

The Download dialog box appears:



At the top of the dialog box is the Account number you will be downloading. There are also checkboxes in the dialog

box that tell you what information you will be downloading. These checkboxes will be checked according to the system options you have changed. If there are specific options you want to download that have not been selected automatically, you can select them now by clicking in the applicable checkboxes.

**2. Click *Start*.**

The database download will proceed. The status bar at the bottom of the dialog box will track the progress of the download.

## ***Configuring the DCM***

If you at any time you want to change the default settings of the DCM provided by the template, or you want to expand on these settings, PassPoint provides a list of function for you to choose from. Using these functions, you can configure your system DCMs in various ways.

DCMs are configured using the DCM Setup dialog box. To reach this dialog box:

**1. From the Config Menu, select *Hardware*.**

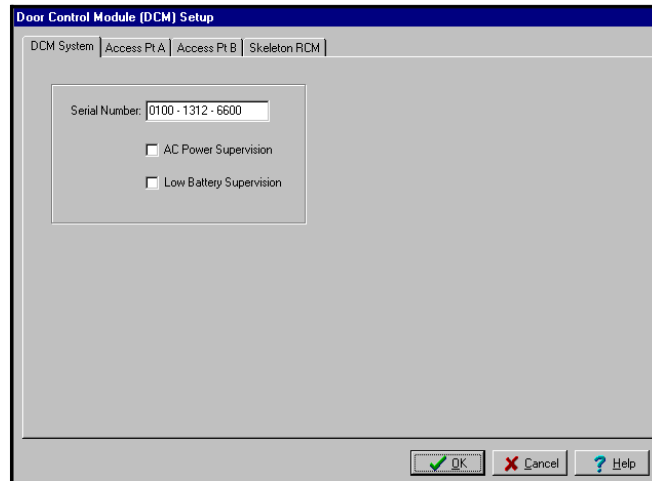
The Installation Configuration dialog box appears.

**2. Right-click on the DCM once.**

This will bring up a menu of option.

**3. From the menu, select *Properties*.**

The DCM Setup dialog box appears:



### ***Using the DCM Setup dialog box***

As you can see, the dialog box contains four tabs. Each of these four tabs contain fields that describe/control various functions and settings of the DCM. Each of the tabs and their related fields are described below.

#### ***DCM system tab***

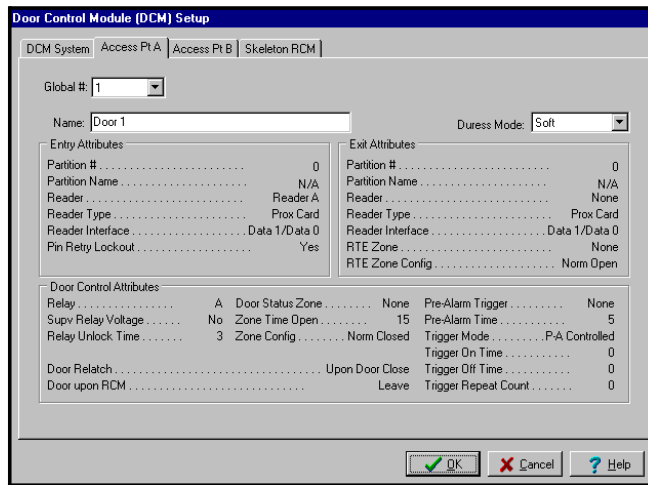
**Serial Number** - You can enter the serial number for this module if you know it or leave this field set to 0000-0000-0000 to auto enroll the serial number. The serial number must be unique.

**Module AC Loss Monitor** (Monitor AC Power Flag?) - When this field is enabled, the module will notify the system when it experiences an AC loss condition. An event will be logged when the ac power is lost or restored. This feature should only be enabled on one of the modules powered by the particular power supply.

**Module Low Battery Monitor** (Monitor Low Battery Flag?) - When this field is enabled, the module will notify the system when it experiences a low battery condition. An event will be logged when the low battery condition is detected and/or restored. This feature should only be enabled on one of the modules powered by the particular power supply.

### Access Point A/B tabs

Access point configuration is the specification of the entry and exit controlling devices which are installed at the access point:



Access point configuration also includes information concerning the door locking device and describes the typical timing parameters that govern passage through the access point (such as how long the lock is to operate, how long the door may remain open, etc.). Access point configuration also consists of the access point's name and any other attributes that may need to be specified in order for the access point to operate properly.

From this tab of the DCM Setup screen, three groups of attributes are displayed. On this screen, these attributes CAN NOT be edited. This screen acts as a summary screen. Double-click within one of the groups in order to open up a screen that will allow you to modify the displayed attributes.

Note that if the Global # for the Access Point is set to 0, the following fields will not be displayed since they do not pertain to an unused Access Point.

**Global Access Point Number** - This field selects the number of this resource from the total number of resources available. Use this drop-down list to select from the allowable values. The system will automatically scroll through only the available numbers.

**Name** - Use this textual field to enter a name for the Access Point you are defining.

**Duress Mode** - The PassPoint system provides for special cases of when an individual is being forced to pass through an Access Point. The individual can indicate to the system that they are under duress to enter or exit the premises. This is done by substituting a "0" for their last PIN digit.

For example, if the individual's PIN is "1234," the duress PIN would be "1230." "0" should be easy to remember since it is similar to dialing a telephone operator. When a duress is initiated, a special message is placed in the event log of the PassPoint system. The system may also initiate a call to a security central station.

The system provides three modes of duress operation - Normal, Soft, and Hard. If the duress mode is set to Soft, entry or egress

will be granted regardless of the access privileges of the individual. If the individual normally would not be allowed to pass, the duress would override, and allow the person to pass. In Normal duress mode, the individual will only be allowed to pass if their access privileges would normally allow them to pass. In Hard duress mode, access will always be denied. Note that the use of Hard duress may endanger the safety of people and should only be used in the most severe security applications. Use this drop-down list to select the desired mode of operation.

### ***Entry Attributes***

This group displays a summary of all the properties that describe the mode of entry control for this Access Point.

**Partition number and name** - Two pieces of access point configuration data that describe the access area or partition that an individual enters when they are allowed entry access through the access point.

**Entry Reader** - An input device installed on the entry side of an access point door. At this device, individuals are required to identify themselves to the PassPoint system so that their access privileges may be examined in order to determine if they should be allowed to pass into the protected area. The term is entry reader because in most cases, the device will be a card reader at which a Cardholder must present their ID card. However, the device may be a keypad at which the individual must enter their assigned Personal Identification Number (PIN code) in order to identify his/herself. In some cases, where higher security is required, the entry reader may be a combinational unit which acts as both a keypad and a card reader.

In the PassPoint system, access points are configured on Door Control Modules (DCMs). Since there are two reader input connections on each DCM, the reader that is being used as the entry control reader for the access point must be specified.

Note that if the installer uses a preset access point configuration, the reader input (READER A or READER B - RDRA or RDRB) is automatically assigned and does not need to be edited.

**Entry Reader Type** - This access point configuration option allows the selection of the reader type. There are many types of card readers and keypads available. The selections in this field include keypads, different types of ID card readers (Wiegand, Proximity, or Magnetic Stripe), and combinational units that consist of both a card reader and a keypad. Use this drop-down list to select the appropriate Reader Type.

**Entry Reader Interface** - All the supported readers which can be used by the system can be categorized by two electrical interface styles. The first is Data1/Data0 (Wiegand style) and the second is Clock & Data. The installer must make the appropriate selection. For most readers other than Magnetic stripe card readers, the appropriate selection will usually be Data1/Data0. This information will be specified by the wiring labels on the card reader or keypad device. Select the appropriate Reader Interface method.

**Pin Retry Lockout** - This is a feature that disables the keypad of an entry reader for a specified amount of time after a specified number of improper PIN entries. Pin retry lockout protects the premises from intruders who tamper with a keypad controlled access point because it slows down the process of trying all possible code combinations. The system logs when



Pin Retry Lockout is initiated at an Access Point. To enable this feature select *Yes*.

The amount of time for Pin Retry Lockout is set in the Administration dialog box. To reach this dialog box, select *Admin* from the *Config* menu.

### ***Exit Attributes***

This group displays a summary of all the properties that describe the mode of exit control for this Access Point.

**Partition number and name** - Two pieces of access point configuration data which describes the access area or partition that an individual exits to when the person is allowed to exit through the access point. If the access point exits out of all controlled areas, this field should be set to zero, indicating an "off premises" condition. Use this drop-down list to select the appropriate Exit to Partition.

**Exit Reader** - An exit reader is an input device that is installed on the exit side of an access point door. At this device, an individual is required to identify his/herself to the system so that their access privileges may be examined in order to determine if they should be allowed to pass out of the protected area.

In the PassPoint system, access points can be configured on Door Control Modules (DCM's). Since there are two reader input connections on the DCM, the one that is being used as the exit control reader for the access point must be specified. Note that if the installer uses a preset access point configuration, the reader input (READER A or READER B - RDRA or RDRB) is automatically assigned, and does not need to be edited.

**Exit Reader Type** - There are many types of card readers and keypads available. This access point configuration option allows the selection of the exit reader type. Use this drop-down list to select the appropriate Reader Type.

**Exit Reader Interface** - All the supported readers which can be used by the system can be categorized by two electrical interface styles. The first is Data1/Data0 (Wiegand style) and the second is Clock & Data. The installer must make the appropriate selection. For most readers other than Magnetic stripe card readers, the appropriate selection will usually be Data1/Data0. This information will be specified by the wiring labels on the card reader or keypad device. Select the appropriate Reader Interface method.

**Request To Exit (RTE) Zone** - In installations where an exit reader is not being employed, it may still be necessary for the system to monitor egresses through an access point. This is usually the case when a Door Status Monitor (DSM) contact (or Door Position Sensor) is used and the door may be used by people exiting through the door by manually opening the door. When a DSM is used, if the PassPoint system is not expecting the door to open from the inside when someone leaves, a Request to Exit (RTE or REX) device must be installed.

The RTE device may be a pushbutton on the wall on the protected side of the door or a limited view passive infrared motion detector which is focused on the area immediately in front of the door on the protected side. In either case, the RTE device is wired to an input zone on the Door Control Module. When a person requests exit through the access point, the RTE zone is faulted by pressing the button or tripping the motion detector. The PassPoint system then understands that a person wants to exit through the door. The PassPoint system unlatches

the door locking device, allowing the person to exit through the door. Since the PassPoint system knows that the door was supposed to open, it will automatically disregard the detection of a door open condition.

Because the DCM provides four input zones (ZONE A thru ZONE D - ZONEA thru ZONED), this field is used to indicate the zone that will be used for this purpose. Note that if the installer chooses a preset access point configuration, this field is automatically filled in by the PassPoint System and cannot be edited.

**RTE Zone Configuration** - This setting allows a normally open, normally closed, or end of line supervised zone configuration to be set for the RTE device. This setting must correspond with the contact configuration of the RTE device.

### ***Door Control Attributes***

This group displays a summary of all the properties that describe the mode of door control for this Access Point.

**Relay** - The Door Control Relay is an electronic switch which resides on the DCM and is used to control the flow of electricity to the door locking mechanism. The Door Control Relay is a "form C" dry contact output, which means that it is used to switch a voltage on or off and may be connected as a normally open or a normally closed circuit.

Magnetic door locks are usually connected to the normally closed side of the relay's connections since magnetic locks must be energized in order to hold the door closed. Electronic door strikes are usually connected to the normally open side of the relay's connections, since door strikes usually need to be energized in order to allow the door to open. Note that door

strikes are available in Fail Safe (when power is removed, the door may open) or Fail Secure (the door is latched when power is removed).

Since the locking mechanisms may have implications of life safety, note that when a door strike is selected for an application, local fire codes may govern the type and configuration of the locking device chosen, and the appropriate side of the relay's contacts must be used. Since the DCM contains two relay outputs (RELAY A or RELAY B - RLYA or RLYB), this field allows the selection of which of the two will be used to control this access point's door. If the installer has chosen a preset access point configuration, the selection of the door control relay is filled in automatically and cannot be edited.

**Supervise Relay Voltage** - In situations where a foreign power supply is employed to provide power to the door's locking mechanism, the installer may choose to have the PassPoint system monitor the power supply. This allows the system to notify an administrator when a power supply that is securing a door has failed. Checking this field enables this feature.

If the installer is using the Ademco Access Control's Power Supply, it may not be necessary to enable this feature since the output of the power supply may already be supervised by the DCM.

**Relay Unlock Time** - This is the amount of time, in seconds, during which the Door Control Relay will be energized, allowing the door to open. The door locking device should be wired appropriately to the normally open or normally closed circuit side of the door control relay so that during this time the door may be opened.

**Door Upon RCM** - In the rare event of a Door Control Module losing contact with the rest of the system, it may be desired that a door which has been commanded open (manually or by a timed schedule) be relatched automatically. This setting allows a setting of "latch", which may be used for exterior door for added security, "unlatch", which may be used for interior doors which would pose a nuisance if they were not able to operate properly, or "leave alone", which leaves the door as-is. In most cases, the "latch" setting will be appropriate. This will provide the best security, and individuals who have their cards (or codes) will still be able to pass through the access point if the appropriate Reduced Capability Mode settings have been configured.

**Door Status Monitor Zone** - This setting allows the selection of a Door Status Monitor Zone. This input zone on the DCM can be wired to a door contact so that the PassPoint system can determine if an intruder has forced the door open when it should have been closed. This zone can also be used to determine if a door was opened rightfully but was not closed within a specified amount of time.

Since the DCM provides four input zones (ZONE A thru ZONE D - ZONEA thru ZONED), this field is used to indicate the zone that will be used for this purpose. If the installer chooses a preset access point configuration, this field is automatically filled in by the PassPoint System and cannot be edited. Also, if the door can be manually opened from the inside when people leave, it is necessary to install a Request to Exit device so that egresses do not cause Door Forced Open alarms.

**Zone Time Open** - This is the amount of time, in seconds, that the door is allowed to remain open when access or egress is granted through the access point. If the door remains open

longer than the specified time, a Door Open Timeout alarm is generated.

**Zone Configuration** - This setting allows a normally open, normally closed, or end of line supervised zone configuration to be set for the DSM device. This setting must correspond with the contact configuration of the DSM device.

**Door Relatch** - When a DSM zone is installed at the door, it is possible for the PassPoint system to determine that the door has closed before the amount of time that it was to remain unlatched. In this case, if the door has not been relatched when it closes, the PassPoint system will automatically relatch the door, preventing a late-comer from pushing an unlatched door open. This feature is also called "Anti-Piggybacking." Most often this option is set to relatch when the door is detected as having closed. The "Upon Door Close" setting should be selected when an electromagnetic door lock is used. The "Upon Door Open" setting can be used at access points which are latched by electronic door strikes.

**Pre-Alarm Trigger** - If a door which employs a DSM is held open longer than the specified Door Open Time, the event history will log a Door Open Timeout alarm. In order to prevent inadvertent Door Open Timeout alarms, a sounder or bell may be installed near the access point. This sounder can be used to warn someone who is holding a door open that an alarm condition is imminent. This sounder is called a pre-alarm warning device.

When the access point is configured with a pre-alarm Device, if the door is still open a preset amount of time before the Door Open Alarm would occur, the pre-alarm device is energized, giving an audible (or even visible) warning to the person

holding the door. Pre-alarm warning devices are usually piezoelectric sounders. P/A devices are driven by one of the two available trigger outputs of the DCM. Each DCM trigger output is an open-collector configured driver, which has a series resistance of 680 Ohms. When energized, trigger outputs will sink current. If a 12 Volt piezo sounder is used, its positive connection should be wired to a source of 12 Volts (with a ground common to the PassPoint system's ground) and its negative connection should be connected to the appropriate trigger output of the DCM. When the P/A warning is in effect, the sounder is energized. Since there are two trigger outputs on each DCM, the appropriate one must be chosen (TRIGGER A or TRIGGER B - TRIGA or TRIGB). Since pre-alarm devices are optional, they are never pre-assigned by the PassPoint system and must be selected by the installer.

**Pre-Alarm Time** - This is the amount of time, in seconds, before the invocation of an access point Door Open alarm at which the pre-alarm device will be energized. For example, if the door is set to be allowed to remain open for 30 seconds, an appropriate pre-alarm time would be 10 seconds, giving 10 seconds of warning to someone who is holding the door open. If the door is still open at the end of the 30 seconds, a Door Open Timeout Alarm Event will occur. The pre-alarm device will remain energized (depending upon its mode) until the door is closed, clearing the Door Open Timeout Alarm.

**Trigger Mode** - The pre-alarm trigger output mode can be set to "Controlled", "One-Shot", or "Repeating". A Controlled pre-alarm trigger will become energized and stay energized until the door is closed. A One-Shot pre-alarm trigger will energize once for the specified On Time, then shut off. A Repeating pre-alarm trigger output will cycle on and off for the specified amount of On Time, Off Time, and for the specified number of

Repeat Counts. If the Repeat Count is set to zero, the cycling will continue until the door is closed. Note that regardless of the mode, the trigger will turn off as soon as the door is closed.

**Trigger On Time** - This is the time, in seconds, that the pre-alarm trigger will remain energized if its mode is set as One-Shot. If the mode is set as Repeating, this is the time that will make up the "On" time of a repeating cycle.

**Trigger Off Time** - This is the time, in seconds, that the pre-alarm trigger will remain de-energized if its mode is set as Repeating. This is the time that will make up the "Off" time of a repeating cycle.

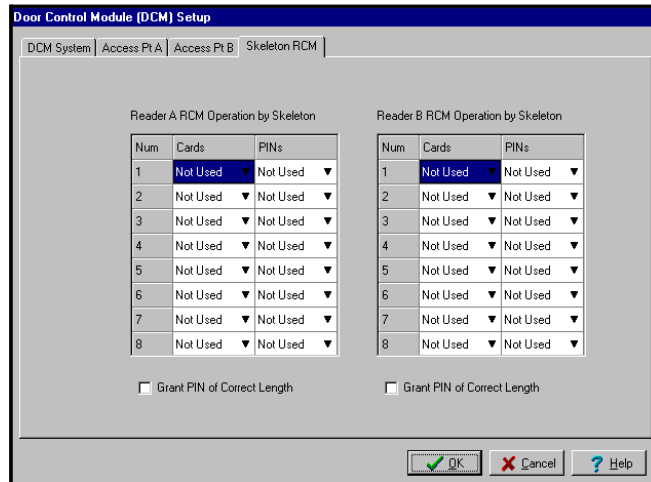
**Trigger Repeat Count** - This is the number of repeated On/Off cycles that will be expressed by the pre-alarm trigger output. If this number is set to 0, the trigger will repeat continuously until the door is closed.

### ***Skeleton RCM tab***

In the rare event of a DCM becoming "disconnected" from the rest of the PassPoint system, the DCM can be told how to act while it is out of contact. When it is "out of contact," the DCM is placed in Reduced Capability Mode (RCM). Note that security is not compromised if RCM mode is configured properly. First, each access point can be selected individually to latch, unlatch, or remain as-is when RCM mode is invoked. This allows perimeter doors to be secured while interior or safety zones can be free to open. Cards and PINs can still be used at the card readers and keypads of the DCM in RCM mode. In most cases, skeleton cards or skeleton PINs can be configured which can be used to unlatch the door for a single cycle or for extended periods of time. Skeletons can also be used to relatch the door. Skeleton cards are configured by



describing the patterns present in the card's electronic signature. Skeleton PINs are configured by allocating special PIN codes that invoke these features.



For each skeleton card/PIN code, select its function. Each card/PIN can have one of three functions:

- **Grant access**
- **Unlatch Indefinitely**
- **Latch Indefinitely**

Grant Access will act similarly to a normal access cycle. Unlatch Indefinitely unlatches the door until commanded otherwise. Latch Indefinitely will latch the door until commanded otherwise. The latch and unlatch functionality can be used by a system administrator who, when the system fails, intends to allow free passage throughout the day until either the end of business, when the latch card (or PIN) is used, or until the system is returned to service.

The type of skeleton code you can enter for an access point depends upon the type of reader you've configured for it. If the access point has only a card reader, for example, you will only be able to configure skeleton cards, not PIN. If you have a combination unit at the access point, you can configure both type of skeleton codes.



---

**Important:** In this area you are only configuring the function for the skeleton code. The actual card/PIN numbers for skeleton codes are assigned in another area of the program, "System-wide Options," discussed in the *PassPoint Express* User's Guide.

---

**Grant PIN of Correct Length?** - Enabling this function disables the use of skeleton PINs. It can only be used at access points that use a keypad for access or egress. Turning on this feature reverts the system to a very low security access point. All that is necessary to gain passage is to enter the correct number of PIN digits. The actual digits that are used does not matter. Any sequence of digits of the correct length will suffice.

Chapter

# 8

## *Adding a Card Enrollment Kit*

Adding a Card Enrollment Kit (CEK) allows you to quickly add ID cards to your system. Cards are enrolled into the system by swiping them at a desktop card enrollment station.

In this chapter you will learn how to:

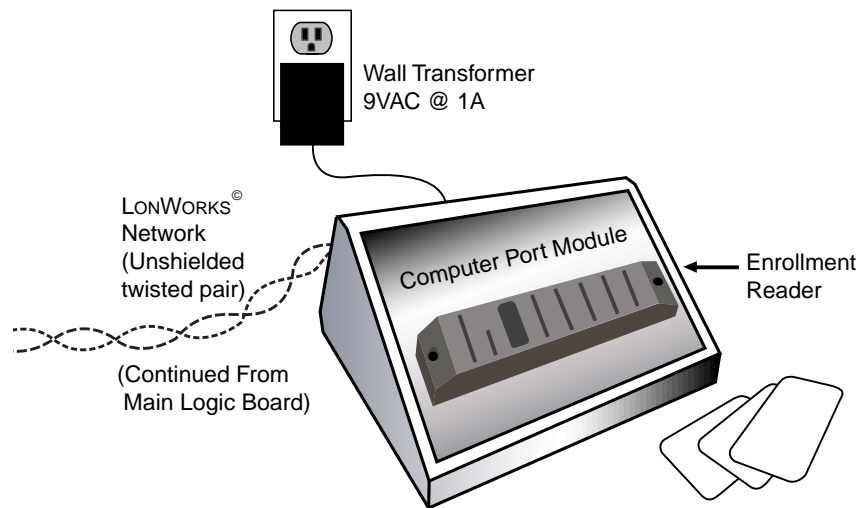
- **Wire all of the components of the CEK**
- **Activate and set up the CEK**
- **Enroll the CEK into an existing PassPoint system**

---

## ***Understanding Your Card Enrollment Kit***

The PassPoint Card Enrollment Kit (CEK) is a self-contained system module that can be added to an existing PassPoint installation in order to make the management of cards (including card enrollment) as simple as possible. Essentially, the CEK consists of a desktop enrollment reader (shown below). System administrators can swipe ID cards at this reader to quickly enroll them in the system.

The CEK connects to the PassPoint system like any other system module, using a twisted pair network connection. It receives power from a 15VDC wall pack transformer.



**CARD ENROLLMENT KIT (CEK)**

**What's in your  
Card Enrollment  
Kit?**

The PassPoint CEK is a kit the includes the following:

- **1 Desktop case, containing,**
  - Computer Port Module (PTCPM)
  - Proximity reader, for card enrollment (PTPROX)
- **1 twisted pair network cable**
- **1 plug-in transformer**

## ***Installing the CEK***

There are six simple steps that must be completed in order to install and enroll the CEK into an existing PassPoint system. Follow each of the steps below and follow the wiring diagram provided.

### ***Step 1 - Choose a location for the CEK***

The CEK is essentially a stand-alone unit. That is, it can be placed on a desk or any other convenient work area. However, the CEK must be located near the system PC, since this is where card enrollment takes place. The administrator will need easy access to both the PC and the CEK when enrolling cards.

### ***Step 2 - Connect the CEK to the system***

Connecting the CEK to the system simply means wiring the CEK into the existing twisted pair network. To do so, follow the steps below and refer to the connections diagram provided:

- 1. Connect the “plug end” of the network cable into the**

**socket of the enrollment reader labeled *NETWORK*.**

The twisted pair network cable supplied with the CEK has two ends. One end contains a two-prong plug. This is the end that gets connected into the enrollment reader.

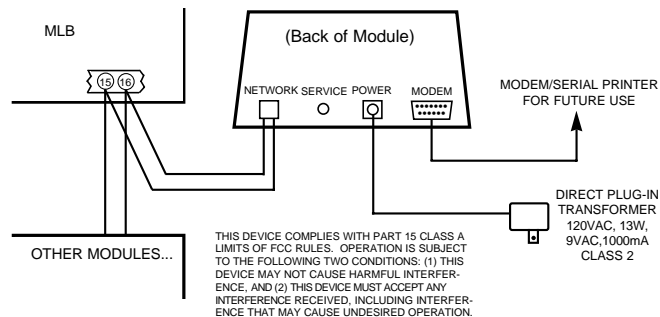
- 2. Connect the two leads on the other end of the network cable to terminals 15 and 16 of the MLB.**

Either lead can be connected to either MLB terminal.

### ***Step 3 - Connect the power transformer and activate the system***

The CEK comes with a wall pack power transformer to be connected between the enrollment reader and a power source.

- 1. Connect the applicable end of the power lead into the socket of the enrollment reader labeled *POWER*.**
- 2. Plug the transformer into a suitable power source and activate the system.**



### **Card Enrollment Kit Connections**

---

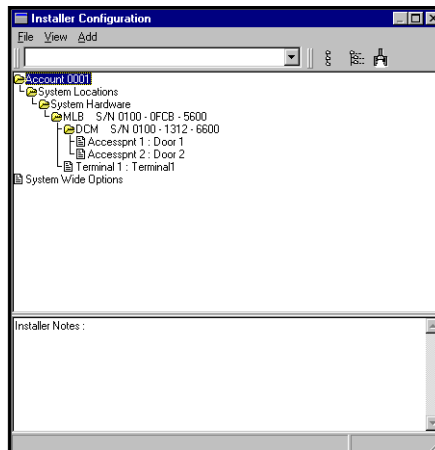
## Step 4 - Add and set up the CEK

Now that the CEK is powered up, you must add the new module (CPM) to your existing installation. To add and set up the new CPM, follow the procedure below:

**1. From the *Config* menu, select *Hardware*.**

The Installer Configuration dialog box appears:

*Use the Installer Configuration dialog box to view/modify system components and to set various system options.*



The Installer Configuration dialog box lists all of the components of the system. Here is where you add new system modules.

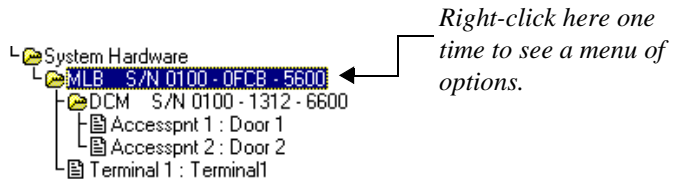


---

Once you make changes in this screen, the changes must be downloaded to the system database in order for them to take effect.

---

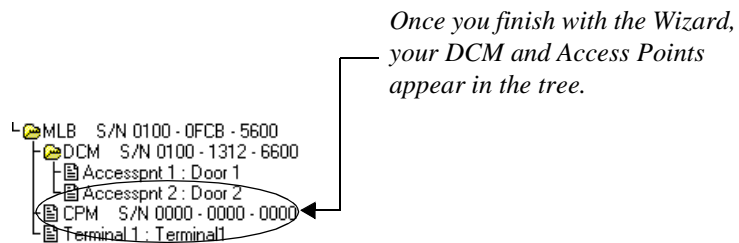
**2. Right-click on the MLB once.**



This will bring up a menu of options.

**3. From the menu, select *Add CPM*.**

The tree in the Installer Configuration dialog box will now show your new CPM:



Now you must enroll the CPM into the PassPoint system so that the system recognizes the device and all its configuration settings. Enrolling the CPM is covered in the next step.

## **Step 5 - Auto enroll the CPM**

Whenever a new module is added to the system, it must be enrolled. Enrolling simply informs the system database that a new system module is present.

When you enroll a system module, the system goes out and searches for any modules connected to it that have not been enrolled. It knows which modules are not enrolled because

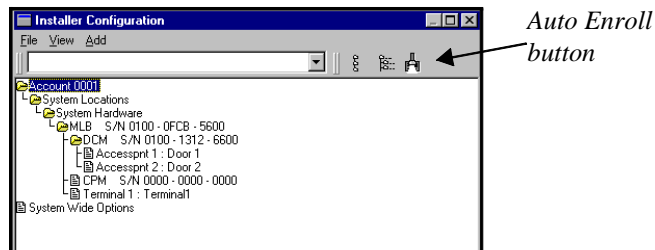


these modules have serial numbers that begin with 0000. For instance, look at the CPM you have just added with the Wizard. It has a serial number that begins with 0000. That means that it has not been enrolled, and is not truly part of the system yet.

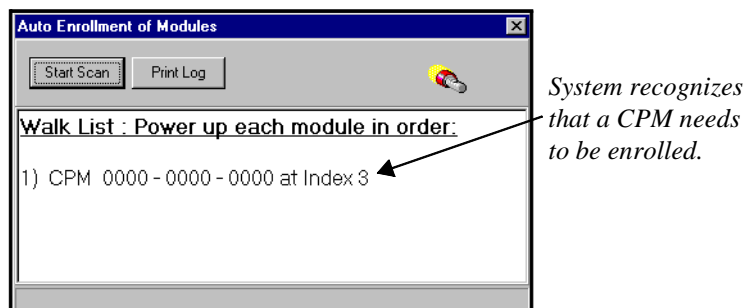
To enroll the CPM you just configured, follow the procedure below:

**1. Click the Auto Enroll button on the Installer Configuration dialog box.**

Refer to the diagram below for the location of the Auto Enroll button:



Clicking this button brings up the Auto Enroll dialog box, shown below:



The enrollment process is all done **automatically** once you click *Start Scan*. The entire process will not take more than a few moments.

**1. Click the *Start Scan* button.**

The system will go out and search for the CPM. When it finds it, a message will appear saying that the CPM has been enrolled.

The system will stop scanning for modules. If you had been enrolling more than one module, you would have had to wait until the system told you that all the modules had been enrolled.

## ***Step 6 - Download the database***

The last step in getting your CEK operational is to download the database.



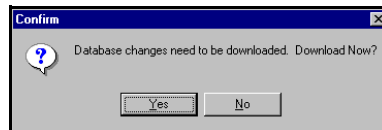
---

Remember, the PassPoint system database resides on the MLB. Here is where all of your system configuration data is stored. However, when you make changes on your PC, these changes are not automatically made to the database on the MLB. They are kept in a temporary storage area on your PC until you download them to your MLB database. Any changes made on the PC must be downloaded to the database in order for them to take effect.

---

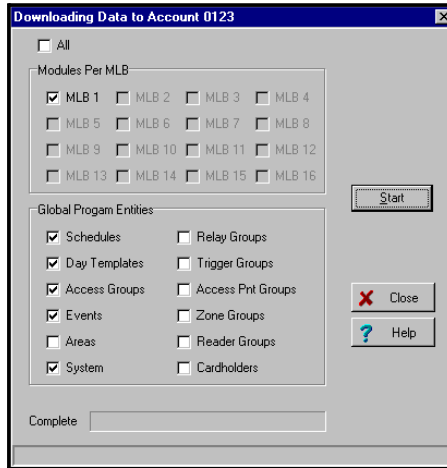
**1. Close the *Installer Configuration* dialog box.**

At close, the system will automatically ask you if you want to download the database:



**2. Click *Yes*.**

The Download dialog box appears:



At the top of the dialog box is the Account number you will be downloading. Make certain that you are downloading to the correct account. There are also checkboxes in the dialog box that tell you what information you will be downloading. These checkboxes will be automatically checked for you according to the system options you have changed. If there are specific options you want to download that have not been selected automatically, you can select them now by clicking in the applicable checkboxes.

**2. Click *Start*.**

The database download will proceed. The status bar at the bottom of the dialog box will track the progress of the download. This may take several minutes, depending on the size of your database.



Appendix

A

## *Wiring Considerations*

When installing your PassPoint system, there are several wiring factors that need to be considered. This appendix explains the various wiring topologies and provides details about wiring specifications.

---

## ***Wiring Considerations***

Before selecting sites for your various system cabinets, you should understand how the system is wired together.

All system modules communicate with the Main Logic Board via a twisted pair network technology. This connection supports communications with up to 126 peripheral modules. Each module connected to the network is considered a “node.” If you are using a PassPoint Access Starter Kit, you have two nodes: an MLB and a DCM, both of which have their own serial numbers. You can, however, expand your system by adding additional nodes. For example, you can add another DCM to control two more Access Points.

When wiring the system and selecting installation sites for your components, there are several factors you must keep in mind. These factors are described on the following pages.



---

The wiring method and installation locations recommended in this manual are in accordance with the National Electrical Code ANSI/NFPA 70.

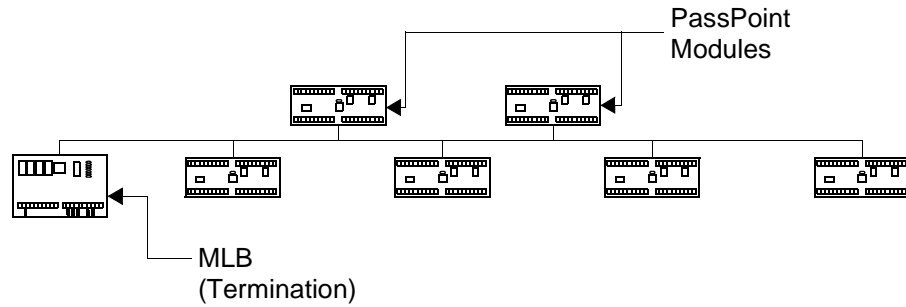
---

### ***Topology***

The system’s unshielded twisted pair wiring technology is designed to support free-topology wiring, and will accommodate bus, star, loop, or any combination of these topologies. PassPoint modules can be located at any point along the network wiring. This capability simplifies system installation and makes it easy to add modules if the system ever

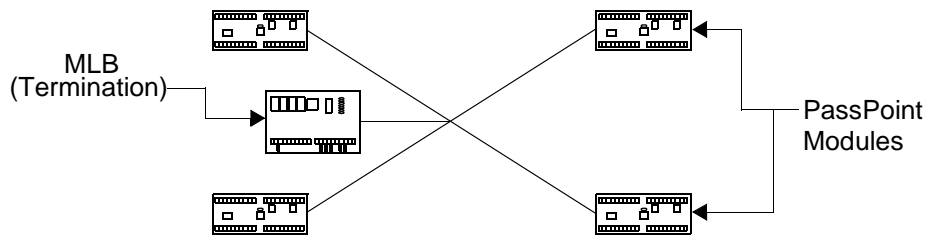
needs to be expanded. The five different wiring topologies are represented in the following diagrams.

*This wiring topology is terminated at the MLB using a 52.3 ohm resistor across the network terminals (15 & 16) of the MLB.*



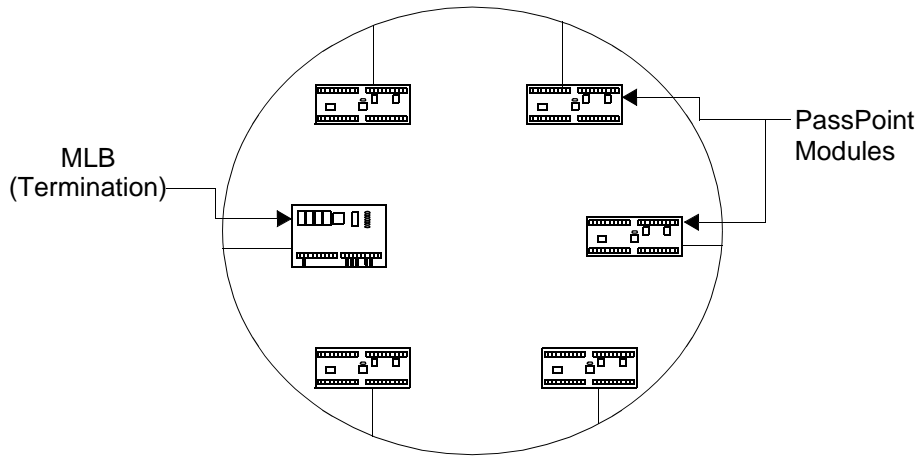
### Singly Terminated Bus Topology

*This wiring topology is terminated at the MLB using a 52.3 ohm resistor across the network terminals (15 & 16) of the MLB.*



### Star Topology

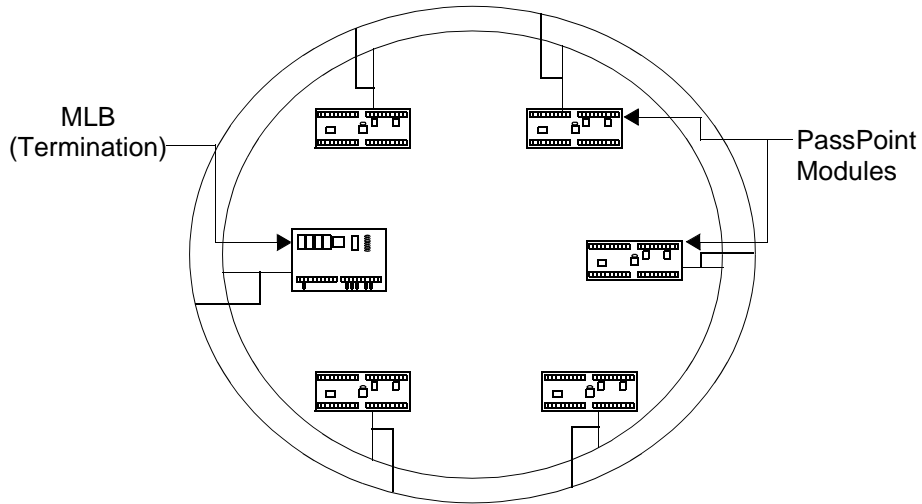
*This wiring topology is terminated at the MLB using a 52.3 ohm resistor across the network terminals (15 & 16) of the MLB.*



### **Loop Topology**

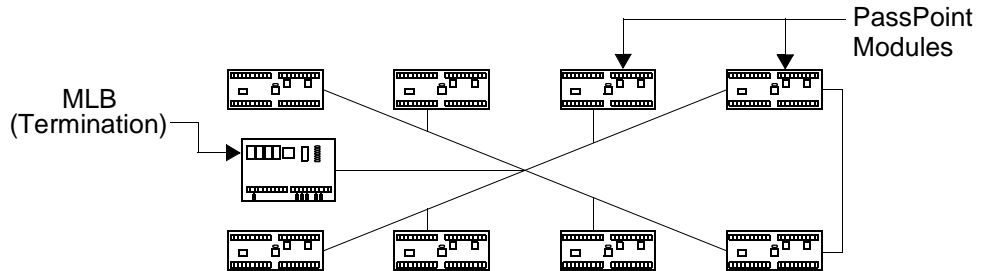


*This wiring topology is terminated at the MLB using a 52.3 ohm resistor across the network terminals (15 & 16) of the MLB.*



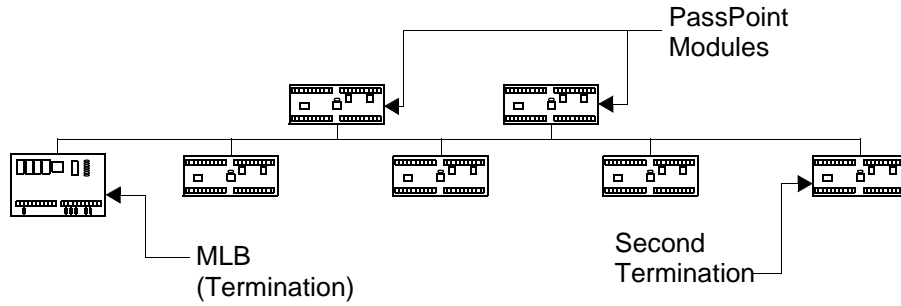
### Redundant Loop Topology

*This wiring topology is terminated at the MLB using a 52.3 ohm resistor across the network terminals (15 & 16) of the MLB.*



### Combination Loop/Bus Topology

*This wiring topology is terminated using a 105 ohm resistor across the network terminals of the two farthest modules. The MLB does not have to be one of the termination sites.*



### Doubly Terminated Bus Topology

Free-topology specifications:

(Can be singly terminated bus, star, loop, or loop/bus combination)

**Table 1:**

| Cable Type       | Max. node-to-node distance | Max. total wire length |
|------------------|----------------------------|------------------------|
| Belden 85102     | 1500 feet                  | 1500 feet              |
| Belden 8471      | 1500 feet                  | 1500 feet              |
| Level IV, 22 AWG | 1500 feet                  | 1500 feet              |

**Doubly terminated bus specifications:**

| <b>Cable Type</b> | <b>Max. bus length</b> |
|-------------------|------------------------|
| Belden 85102      | 8000 feet              |
| Belden 8471       | 8000 feet              |
| Level IV, 22 AWG  | 4000 feet              |

---



When planning your wiring scheme, keep in mind that using shielded wiring will drastically reduce the allowable wire run lengths.

---

**RS-232 cabling:**

Standard, 9-conductor, shielded, 22 AWG cable, 32 feet (null modem)

**Keypad wiring:**

22 AWG, 3 feet

(The keypad should be mounted on the cabinet only and not wired through the premises.)

**Power Harness:**

Use power harness SA12160 only (supplied). (Local and remote power outputs of power supply.)

**Door strike power:**

Depends on wire gauge and current requirements of the door

strike or magnetic lock. Probably about 500 feet of 16 AWG wire for 350 mA of current.

**Reader interfaces:**

200 feet of 22 gauge

300 feet of 20 gauge

500 feet of 18 gauge

## ***Wiring notes***

Keep reader, Echelon, and RS-232 wiring away from any high-current wiring. This includes the door strikes, as well as any building wiring that delivers power to “noisy” load (AC units, refrigerators. etc.).



---

We suggest using an electric suppressor such as EL-EDS (manufactured by EDCO) to provide transients protection for magnetic locks/door strikes and relay contacts. Install the suppressor as close as possible across the leads connected to the leads lock.

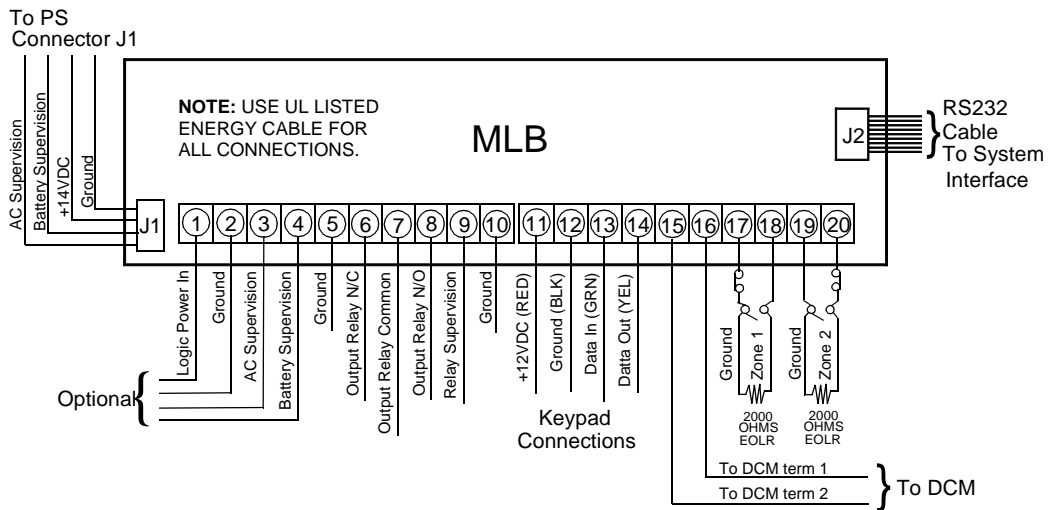
---

**Wire characteristics:**

| <b>Cable Type</b>                                                                    | <b>Wire Dia./<br/>AWG</b> | <b>Rloop<br/>Ohm/km</b> | <b>C<br/>nF/km</b> | <b>Vprop<br/>% of c</b> |
|--------------------------------------------------------------------------------------|---------------------------|-------------------------|--------------------|-------------------------|
| Belden 85102<br>Single twisted pair,<br>stranded 9/29,<br>unshielded, plenum         | 1.3mm/<br>16AWG           | 28                      | 56                 | 62                      |
| Belden 8471<br>Single twisted pair,<br>stranded 9/29,<br>unshielded, non-ple-<br>num | 1.3mm/<br>16AWG           | 28                      | 72                 | 55                      |
| Level IV 22AWG<br>Single twisted pair,<br>typically solid &<br>unshielded            | 0.65mm/<br>22AWG          | 106                     | 98                 | 41                      |
| JY (St) Y 2x2x0.8<br>4 wire helical twist,<br>solid, shielded                        | 0.8mm/<br>20.4AWG         | 73                      | 98                 | 41                      |

# Main Logic Board Connections

Wire the MLB according to the diagram below:

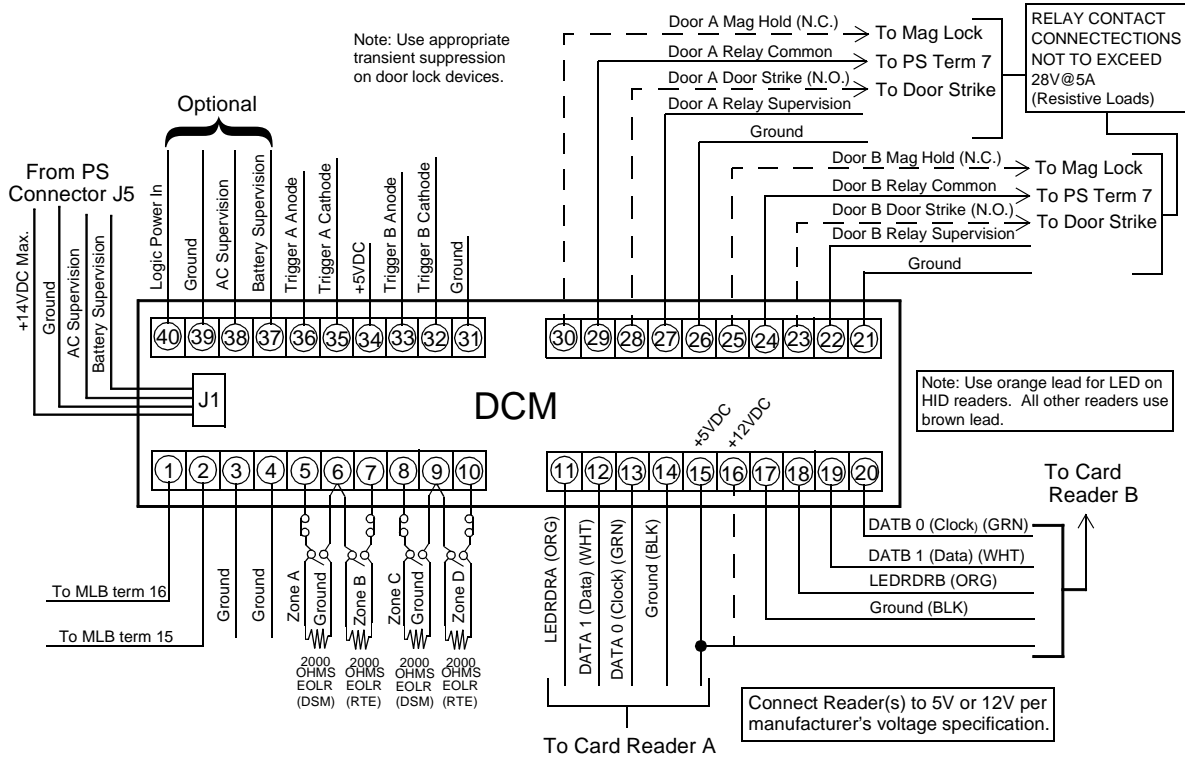


MLB Battery Support Ademco Part Number N7673. 3V Lithium Battery estimated standby lifetime: 10years.  
**CAUTION** - Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries in accordance with the manufacturer's instructions. Battery type: Lithium battery type 2025.

THIS EQUIPMENT SHOULD BE INSTALLED IN ACCORDANCE WITH THE NATIONAL FIRE PROTECTION ASSOCIATION'S STANDARDS 70 & 74 (NATIONAL FIRE PROTECTION ASSOC., BATTERYMARCH PARK, QUINCY, MA, 02269). PRINTED INFORMATION DESCRIBING PROPER INSTALLATION, OPERATION, TESTING, MAINTENANCE, EVACUATION PLANNING AND REPAIR SERVICE IS TO BE PROVIDED WITH THIS EQUIPMENT.

# Door Control Module Connections

Wire the DCM according to the diagram below:



---

## ***Power supply specifications***

Transformer part number N8167:120VAC PRIM. (60 Hz)  
18VAC 50VA SEC.

**Note:** Connect transformer to 24-hr. wall outlet.

Switching Regulator Output: 13.3V +/- 1.2VDC  
@ VAC Input: 102V-132V  
Vripple 600mVpp

Linear Regulator for Local  
Power Output: 13.7VDC @ 450mA

Total Power Supply  
Output Current: 1.8A +/- 200mA

Door Strike/Mag Lock  
Max. Current: 900mA

J1 Local Logic Power Output: 450mA max.

J5 Logic Power Output: 450mA max.



---

Connection to terminal blocks 9 and 10 is not required for AC and battery supervision when power harness SA12160 is used with J1 and J5. If SA12160 power harnesses are not used, connect Low Battery and AC Loss supervision terminals from power supply to Low Battery and AC Loss supervision terminals of system modules. AC Loss and Low Battery supervision outputs provided for supervision of maximum two PassPoint modules.

---



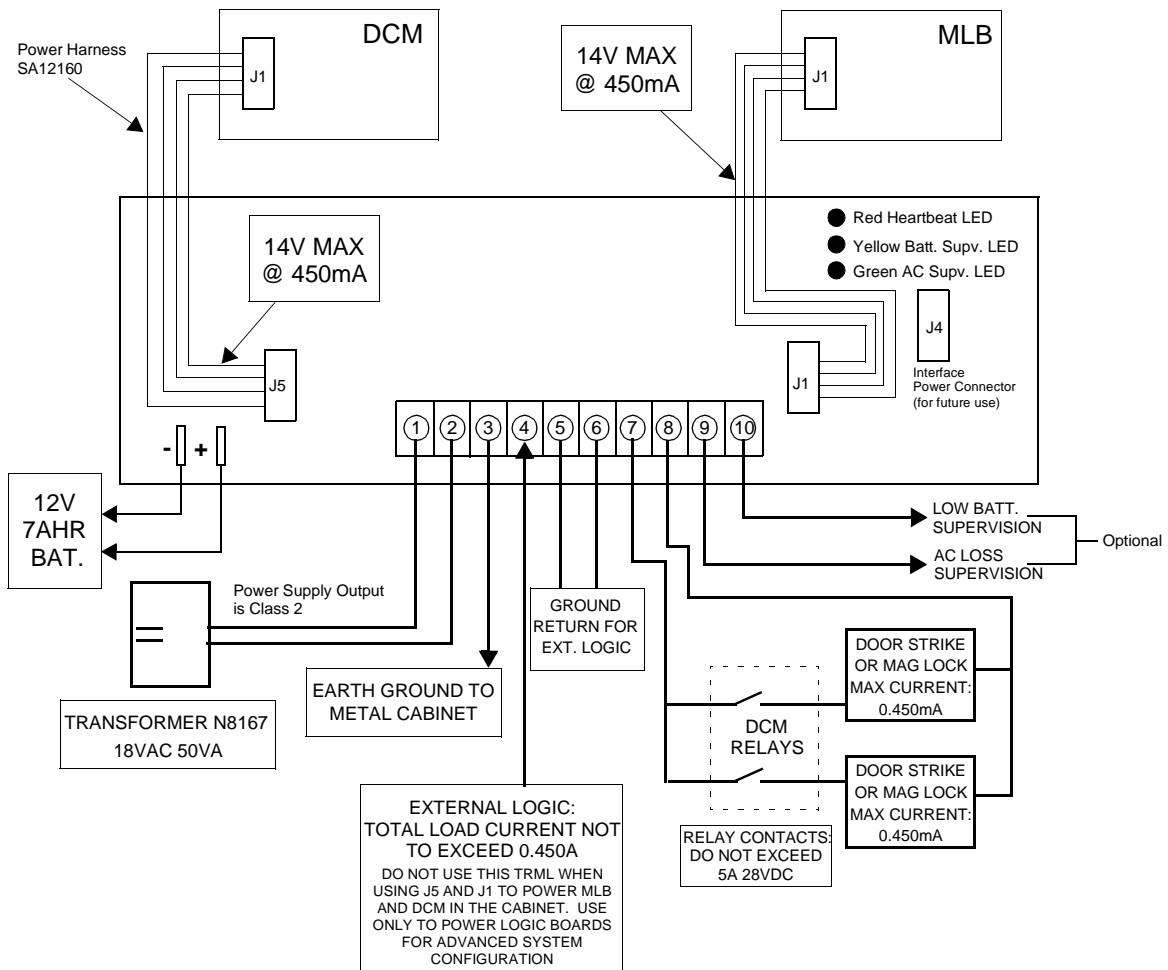
**System Status Indicators:**

AC Loss LED: Green

Low Battery LED: Yellow

Heartbeat LED: Red

Battery Backup: 12V/7AH



## Power Supply Current Distribution and Load Connections

## Glossary

# G

## *Access Control Glossary*

### A

**Access Card** - A card, generally the size and shape of a credit card, containing encoded data. The data can be encoded in a variety of ways, sometimes including more than one encodation technology. (See Magnetic Stripe, Wiegand, Proximity.)

**Access Control** - Allowing the right person through the right doors at the right time based on: 1) What they Have, 2) What they Are, and/or 3) What they Know.

**Access Group** - A group of individuals that share common access privileges. That is, associated Access Points (doors) and times. The Access Group defines the access privileges of the individuals. All members of an Access Group have identical access privileges.

**Access Level** - See Access Group

**Access Partition/Access Area** - A completely enclosed space that is controlled for entry and egress. Generally, when a person passes into the area, PassPoint will note that the person is in the specified area. In this way, the system can keep track of where people are within a facility. Note, however, that both

entry to and egress from the area must be logged by the PassPoint system in order for this feature to work. That is, if the entry to an area is controlled by PassPoint but egress is not controlled by PassPoint, the system will not be notified when a person leaves the area. This will lead to incorrect occupancy reading of the protected areas.

**Access Point** - A collection of card readers, zones, triggers, and relays committed to the control and monitoring of the door control hardware at a single point of passage.

**Access Privileges** - The rights allocated to an individual which define his/her access capabilities. Access privileges consist of the specifications of when and where a person may gain access or be allowed egress from a controlled area.

**Anti-Passback (APB)** - An Access Control function whereby a cardholder is prevented from “passing back” his card to another person to gain entry into the same area twice, without leaving. A parking garage would be a good example of such a situation. A boss may try to pass his card back to his secretary, so that they may both park in the executive parking lot. Facilities are typically fitted with both Entry and Exit readers when Anti-Passback is implemented. A cardholder must alternate usage between entry and exit readers. If the cardholder attempts to pass through an entry reader twice consecutively, the cardholder will generate an Anti-Passback violation. In addition, based on the configuration of the Access Control System, he may be denied access as a result of that violation. In ADEMCO’s implementation, it simply means attempting to use the same Access Point in the same direction within a specified period of time. (See also: Hard Anti-Passback, Soft Anti-Passback)

**Archive** - A file stored on your system's PC that holds previously uploaded events. Archives allow you to keep and organize all of the events recorded by your system.

**Arm Away** - This is a function of the burglary sub-system of the PassPoint system. Arming the system enables zones to cause a burglary alarm. Arming the burglary sub-system in the Away mode enables Interior, Perimeter, and 24 Hour zone types so that they will cause an alarm when faulted.

**Arm Stay** - This is a function of the burglary sub-system of the PassPoint system. Arming the system enables zones to cause a burglary alarm. Arming the burglary sub-system in the Stay mode enables only the perimeter and 24 Hour zones types.

**B**

**Biometrics** - Readers that identify human attributes such as fingerprint, hand geometry, voice recognition, or retinal scans. (What you are)

**Bypass (Access Point)** - When an Access Point is placed in Bypass mode, the locking mechanism is unlocked, no forced door or door open too long alerts are generated, and any requests to exit are ignored (the door is already unlocked). The access control industry also refers to this condition as "Free Access".

**Bypass (Zone)** - When an alarm zone is placed in Bypass mode, it no longer generates alerts to the user when the zone changes state. You may want to Bypass an internal zone (such as a corridor) during the day, when you would expect activity, but no security violations are actually occurring.

**C**

**Card Reader** - A device used by CardHolders to identify themselves to the PassPoint system. The card reader reads the

CardHolder's access card so that the access privileges of the CardHolder may be examined in order to determine if the CardHolder should be allowed to pass into the protected area. In some cases, the device used for identification may be a keypad rather than a card reader. Instead of presenting a card to the keypad, the CardHolder must enter their assigned Personal Identification Number (PIN code) in order to identify his/herself. In situations where higher security is required, the entry reader may be a combination unit which acts as both a keypad and a card reader.

**Cardholder** - An occupant of a premises who has been issued an access card or access code (or PIN, Personal Identification Number) which is used to request passage through protected Access Points within the premises.

**Committed Resource** - A resource, such as a reader or relay, that is directly assigned to an Access Point. The committed resource can no longer be controlled or monitored as an individual item. A committed relay, for example, is used to control the door to which it is assigned.

**CPM (Computer Port Module)** - The CPM acts as an PassPoint network-to-RS232 interface. It will permit a connection for a PC or printer, in addition to an enrollment reader. The enrollment reader cannot be committed to an Access Point.

## **D**

**Day Template** - The part of a time schedule that is used to specify time intervals during the day that an action can occur. Day templates contain time "windows" that define start and stop times for actions. For example, A Day Template could contain the following time intervals or "windows": 07:00-08:30, 12:00-13:00, 17:00-17:30. This Day Template could

then be assigned to Monday through Friday of a schedule, and the schedule could then be assigned to a scheduled action upon window opening or closing. That action could be to bypass an Access Point during normal workdays. (See also: Schedules)

**DCM (Door Control Module)** - The DCM provides all the inputs and outputs required to manage one or two Access Points (i.e. doors). This may also be a single Access Point where Anti-Passback is implemented.

**Deny Override** - This function allows all cards to be granted access. When a system is initially installed, this feature can be enabled to allow all people to access all doors. The event history can then be reviewed and the configuration fine-tuned. After a week or so of careful monitoring, the feature can be disabled, and standard control can be enforced.

**Disarm Away** - This is a function of the burglary sub-system of the PassPoint system. Disarming the system disables zones from causing a burglary alarm. Disarming the burglary sub-system in the Away mode disables Interior, Perimeter, and 24 Hour zone types so that they will not cause an alarm when faulted.

**Disarm Stay** - This is a function of the burglary sub-system of the PassPoint system. Disarming the system disables zones from causing a burglary alarm. Disarming the burglary sub-system in the Stay mode disables only the perimeter and 24 Hour zones types.

**Door Control Relay** - The Door Control Relay is an electromechanical switch which is used to control the flow of electricity to the door locking mechanism. The Door Control Relay provides a “form C” dry contact set for an output. In this

way it can be used to introduce or eliminate current flow to an external device.

**Door Open Time** - The amount of time a door is permitted to remain open after a valid entry, before an alarm is generated by the access control system.

**Door Strike** - An electromechanical locking device typically installed in a door frame to enable locking and unlocking of the door by electrical or electronic means. Internally, the device consists of a solenoid, to which power is applied, causing a plunger to move linkage which releases a locking mechanism.

**DSM (Door Status Monitor)** - A zone in an Access Control System committed to the monitoring of a door sense switch. The door sense switch will reflect the state of the door (open or closed) and allow the PassPoint to determine if the door has been forced open, or held open too long.

**Duress** - A condition whereby a cardholder may be confronted by an intruder in an effort to gain access to a secure area. The cardholder can “secretly” signal security that he is entering the secure area under “duress” through the implementation of a duress feature.

## **E**

**Enrollment Reader** - A reader (connected to a CPM) which can be used to enroll cards into the Access Control System.

**Entry/Exit Control** - A means of controlling and monitoring the flow of CardHolders through a building. It is used in conjunction with Access Groups to either allow or deny group members access to specific areas, based on their directional usage of Access Points.



**Entry Reader** - An input device installed on the entry side of an Access Point door. At this device, individuals are required to identify themselves to the PassPoint system so that their access privileges may be examined in order to determine if they should be allowed to pass into the protected area. The term is entry reader because in most cases, the device will be a card reader at which a CardHolder must present their ID card. However, the device may be a keypad at which the individual must enter their assigned Personal Identification Number (PIN code) in order to identify his/herself. In some cases, where higher security is required, the entry reader may be a combination unit which acts as both a keypad and a card reader.

**EOLR Supervision (End Of Line Resistor Supervision)** - It may be desirable to know if someone has cut or shorted a cable monitoring a zone, such as a door sense switch. A resistor can be placed in the zone's circuit at the protected point, such that the controller can detect line trouble, in addition to fault and normal conditions.

**Event/Action Relationship** - An option programmed by the user that allows system functions to be linked to a system event. Upon the occurrence of the system event, the action is performed.

**Event Browser** - The PassPoint tool for viewing uploaded events. The Event Browser organizes all of the uploaded events by date and displays them on screen.

**Event Log (or History Log)** - A list of events which indicate the actions performed by and within the PassPoint system. Each event log entry contains the time, date, and any other attributes that specifically define the event.

**Executive Privileges** - An option that can be granted to CardHolders to allow them full access to all of the system Access Points.

**Exit Only** - One of the modes in which an Access Point may be configured to operate. In this mode, the Access Point will only accept exit requests through the Access Point. Any entry reader will be ignored.

**Exit Reader** - An exit reader is an input device that is installed on the exit side of an Access Point door. At this device, an individual is required to identify his/herself to the system so that their access privileges may be examined in order to determine if they should be allowed to pass out of the protected area. (See also: Entry Reader)

**F**

**Facility Code** - An encoded value (within the access card) which can be used to identify the facility or site which a specific group of cards has been issued. This information can be used in a reduced security environment whereby the specific card number is ignored, but anyone from that “facility” can gain access.

**Fail Safe** - A locking device which will automatically unlock in the event of power loss.

**Fail Secure** - A locking device which will automatically lock in the event of power loss.

**Force Arm Away** - Arms the burglary system in the away mode. Any faulted zones will be automatically bypassed.

**Force Arm Stay** - Arms the burglary system in the stay mode. Any faulted zones will be automatically bypassed.

**Forgive (Entry/Exit, Anti-Passback)** - Because Entry/Exit and Anti-Passback violations can result in access and egress denials, Cardholders can be "stuck" in the place where the violation is detected if their card swipes are denied. These functions permit the user "forgive" Anti-Passback and Entry/Exit violations for a Cardholder and/or an Access Point. When these functions are used, the system's Anti-Passback and/or Entry/Exit mechanisms and records are re-synchronized so that Cardholders can continue through the premises.

**Form C Relay Output** - A Form C relay output is a configuration comprised of a Common terminal point, a Normally Open terminal point, and a Normally Closed terminal point. With the relay in a de-energized state, the Common and Normally Closed points are connected to each other, and the Common and Normally Open points are disconnected from each other. When the relay energizes, the Common and Normally Closed points disconnect from each other, and the Common and Normally Open points connect to each other.

**Free Access** - See Bypass (Access Point)

**H**

**Hard Anti-Passback** - If a cardholder is in violation of antipassback rules, he will not be granted access.

**Hard Entry/Exit** - If a cardholder is in violation of Entry/Exit rules, he will not be granted access.

**Holiday** - A component of time schedules that define days of the work week when the “normal” work schedule does not apply to the premises. For example, Thanksgiving day would be considered a holiday.

**K**

**Keypad** - Typically a 12 button arrangement of momentary pushbuttons used to indicate a code to the system based on a specific sequence of key depressions. The keypad will generally resemble a telephone keypad with respect to the relative positions and key name assignments.

**L**

**Locked (Access Point)** - Latches the door of the Access Point. The Access Point's readers will be disabled for access control functions. The Access Point will not allow any accesses or egresses in the Locked mode.

**M**

**Magnetic Stripe** - The black or brown stripe typically found on the back of a credit card. The stripe is encoded similarly to a cassette tape, that is, magnetic domains are impressed upon the material so that it can be read by a reader at a later time. (What you have)

**Mag Lock (Magnetic Lock)** - A large coil of wire mounted to a door frame, which when current is passed through the coil of wire, a strong magnetic field is created. A large metal plate is also secured to the door, and will be held tightly against the coil of wire, due to the presence of the strong magnetic field. The door can be released (or “unlocked”) by interrupting the flow of

current through the coil, thereby removing the strong magnetic field.

**MLB (Main Logic Board)** - The MLB is the main controller of the Access Control System. It contains the card database, the event log, and system configuration information. It also keeps track of the system status. The MLB receives its power from the Access Control power supply, and communicates with the Door Control Module (described above) to determine if access should be granted to a particular Access Point. It can also coordinate the activities of other system modules, such as the QRM or ZIM.

**Modem** - A device that converts digital information into analog information so it can be transmitted over telephone lines, and converted back to digital information at the other end by another modem.

**N** **Name Pool** - A collection of names, assigned by a user, that can be applied to system objects (i.e. relays, readers, etc.) The name pool can contain a maximum of sixty names, each up to fifteen characters in length. This can also be known as “Custom Alpha Descriptors”.

**O** **Outputs** - Auxiliary devices in an access control system that control external devices such as electronic locks, piezo sounders, or light indicators. These can consist of relay outputs (dry contacts) or transistorized outputs (current sinking devices).

**P** **PIN (Personal Identification Number)** - A number assigned to an individual that, when entered in to a keypad, will allow the Access Control System to grant access into a secure area based on a person’s knowledge. PINs can also be combined with

encoded cards and biometric devices to ensure higher levels of security. (What you know)

**Pin Retry Lockout** - A feature that disables the keypad of an entry reader for a specified amount of time after a specified number of improper PIN entries. Pin retry lockout protects the premises from intruders who tamper with a keypad controlled Access Point. It slows down the process of trying all possible code combinations. The system records an event when Pin Retry Lockout is initiated at an Access Point.

**PIR (Passive Infra Red)** - Typically, a sensor device that can sense movement within a specific area and change the state of a set of internal contacts as a result. These contacts can then be wired to a Request To Exit zone on an Access Control System for automated egress when a person approaches an Access Point from inside a protected area.

**Power supply (Access Control)** - The Access Control power supply provides all the power needed by the MLB and DCM. It is connected to the AC line voltage via an 18VAC, 50VA Basler-type plug-in power transformer. The power supply provides a battery backup/charger connection and supports a 7-AmpHour battery. In addition, it has the capability to monitor and test the AC power input and battery condition. The results of which are provided to the modules, and ultimately to the MLB.

**Pre-Alarm Trigger Time (P-A Time)** - This is the amount of time, in seconds, before the start of an Access Point Door Open alarm, at which time the pre-alarm device will be energized. For example, if the door is set to be allowed to remain open for 30 seconds, an appropriate pre-alarm time would be 10 seconds. After the door has been open for 20 seconds, the system would

then give 10 seconds of warning to someone who is holding the door open. If the door is still open at the end of the 30 seconds, a Door Open Timeout Alarm Event will occur. The pre-alarm device will remain energized (depending upon its mode) until the door is closed, clearing the Door Open Timeout Alarm.

**Precedence Level** - A type of authority level that tells the system when certain system resources can be controlled. Simply put, precedence levels determine whether or not a manual operation should take “precedence” over any other previously initiated action.

**Protected** - The normal operating status of an Access Point. When an Access Point is protected, only valid CardHolders can access it.

**Proximity** - A reader technology relying on a radio frequency link between the reader and the card (prox reader and prox card). Encoded information is passed between the card and reader, usually supplying a unique pattern enabling identification of the card holder. (What you have)

**Q**                    **QRM (Quad Relay Module)** - A module that can be placed on the Access Control network to provide four additional Form C, supervised outputs, in addition to four Trigger outputs.

**R**                    **RCM (Reduced Capability Mode)** - In the unlikely event of a DCM (Door Control Module) becoming "disconnected" from the rest of the PassPoint system, the DCM can be told how to act while it is out of contact with the MLB (Main Logic Board). When it is "out of contact," the DCM is placed in Reduced Capability Mode (RCM).

**Reader** - A device that a cardholder presents his access card to, that will read the card's encoded data and transmit it to an access control panel. The panel will then make a decision as to what action to take as a result of that card read (energize a relay, etc.).

**Relay Supervision** - The common pole of the Form C relay will be monitored for the presence of voltage. An alert will be generated if the voltage is not sensed. This might be used to sense if an external power supply (used for lock power) has failed.

**Resource Group** - A collection of system resources all of the same type. Grouping resources allows you to control all the items in the group with one command. For example, if you grouped all of the doors leading to the outside as "Exterior Doors", you would be able to bypass or protect the entire group with one command.

**RTE (Request To Exit)** - A condition generated by a device (push-button, crash bar, PIR, switch floor mat, etc.) that indicates to the PassPoint that someone is leaving the protected area. No card is required, and no forced door event is generated. It can also result in the door unlocking. Other names used in the industry for this condition are: REX, Egress, and Bypass. Note: Do not confuse this usage of bypass with the ADEMCO meaning. (Please see Bypass)

## **S**

**Schedule (or Time Schedule)** - A list of time intervals that can dictate when events or conditions can start, stop, or occur. For example, schedules control when certain Access Groups are allowed access to the premises. Schedules are made up of Day Templates.



**Shunt (Access Point)** - This function disables the DSM zone on the Access Point. The Access Point will then operate as though it does not have a DSM zone installed. This function is useful in instances of hardware failure, when a bad door contact might hinder the operation of the Access Point. The Access Point can be operated in the shunted state until it is repaired.

**Shunt (Zone)** - Shunting a zone serves almost the same purpose as the Bypass function except for one exception. While the Bypass function causes detected changes in zone status to occur without generating any alarms, Shunting a zone causes the zone to go unmonitored. This can be beneficial when there is a malfunctioning zone on a peripheral module. The peripheral module may be flooding the communications network with zone status change messages. Shunting the zone tells the appropriate peripheral module to ignore the applicable zone and stop sending status change messages. The zone can then be kept Shunted until it is repaired.

**Skeleton Codes (or Skeleton Cards)** - Skeleton codes are used to unlock Access Points during Reduced Capability Mode (RCM) operation. They are only used when the communications link between the MLB and its DCM has been interrupted. Under these conditions, the DCM uses these skeleton codes as a very small card database. When the communication link is restored, the skeleton code database is no longer utilized.

**Soft Anti-Passback** - If a cardholder is in violation of antipassback rules, he will be granted access, but a record of the violation will be stored in the event history.

**Soft Entry/Exit** - If a cardholder is in violation of Entry/Exit rules, he will be granted access, but a record of the violation will be stored in the event history.

**Supervision** - That process by which a device is monitored for faulty operation. This is typically accomplished through voltage or resistance monitoring. (Also see: EOLR Supervision and Relay Supervision)

**T**

**Threat Level** - A global condition that can be set by system users to qualify a state of emergency. There are six threat level, TL0 through TL5. TL5 is the highest threat level.

**Time and Attendance** - Information extracted from the Access Control transaction database that can be used by payroll departments to calculate an employee's paycheck.

**Transaction** - An event that occurred within the access control system which generates a record in the stored database.

**Transient Suppression** - A process by which short term, high energy bursts can be limited to safe levels by the use of specialized electronic components. The purpose of this might be to protect sensitive electronic equipment connected over communications lines of considerable length.

**Trigger Outputs** - Trigger Outputs are solid state digital switches (transistors) that can be configured as committed or uncommitted resources. These can be used to illuminate LEDs, activate piezoelectric sounders, energize an external relay, or signal a long-range radio transmitter.

**Trouble** - A trouble condition generally indicates a problematic line (cable or connection) for a supervised zone.

**U**

**User (system)** - A person that interacts with the system through the system interface. Users can control readers, set time schedules, enroll ID cards, etc. There are four levels of users: Installer, Masters, Managers, Operators.

**User Code** - The identification code used by a user to gain access to the system. User codes are entered through the system interface.

**V**

**VGM (Vista Gateway Module)** - The PassPoint component that provides an interface between the Ademco Vista Panel and the Ademco Access Control System.

**Visual Verification** - An optional mode that requires the system to defer to an operator to visually verify the identity of all CardHolders after a CardHolder's card/PIN has already been verified by the system.

**W**

**Walk Test** - This function initiates a manual test of the system's uncommitted zones. Once the option is selected the user should sequentially fault all uncommitted zones in the system. The system will report all faulted and unchanged zones so that the integrity of the system may be verified.

**Watchdog Timer** - An internal circuit within the system that will reset the control electronics in the unlikely event that it becomes locked in an endless loop of some kind. This will allow the system to continue to operate even though there would have ordinarily been a problem that would have caused the system to 'lock up' or freeze.

**Wiegand** - A card reader technology relying on a series of wires imbedded in a vinyl card. The Wiegand card is passed through a Wiegand reader to communicate a distinguishing

pattern of ones and zeroes to the access control system to identify a particular card holder. (What you have)

**Windows (Time)** - A time interval during a the day when actions are allowed to occur. Up to eight of these time windows can be contained within one Day Template.

**X** **XX Minutes Timer** - A timer that is programmed on the Vista Alarm Panel that expires after a preset number of minutes. Generally, a Vista Output Relay may be configured to operate for the duration of the timer. This timer can be programmed at location 1\*74 on the Vista Panel.

**Y** **YY Seconds Timer** - A timer that is programmed on the Vista Alarm Panel that expires after a preset number of seconds. Generally, a Vista Output Relay may be configured to operate for the duration of the timer. This timer can be programmed at location 1\*75 on the Vista Panel.

**Z** **ZIM (Zone Input Module)** - A module that can be placed on the Access Control network to provide eight additional zone inputs, which can be configured as supervised or unsupervised.

**Zone** - An area or object being protected by an electronic circuit.